Cloud Transformation

Kamala Manju Kesavan

Received: Revised: Accepted: Published:

Abstract - Cloud transformation is a pivotal tool that redefines an organization's operations and strategy. It is a comprehensive process of migrating an organization's operations data, applications, and software to the cloud platform. The process involves optimizing and modernizing an organization's model, security, data management, and analytics to align with its objectives in digital transformation and tapping on data governance solutions to drive the process of decision-making [11].

1. Introduction

The digital economy continuously expands, and an organization's digital prowess is synonymous with success. Correspondingly, cloud transformation incorporates the digital adoption of new technologies that enable an organization to adopt new ways of working and quick response to threats. Cloud transformation fundamentally shifts an organization's operations, culture, and technology. It emerges as a keystone that enables organizations to stay agile and competitive.

Benefits and Challenges

As an organization leveraging cloud transformation strives to be more responsive and agile in the current digital landscape. Cloud transformation provides compelling advantages that drive them to embrace this transition among various challenges. Cloud transformation benefits play out as illustrated below;

2. Cost Efficiency and Scalability

Costs Reduction. Migrating to clouds shifts an organization's capital expenditures model to operational expenditures. This shift offers an organization more manageable and predictable costs since it does not need to invest in expensive infrastructure and hardware [7]. They get to pay expenses that arise from what they use.

Scalability and Flexibility . The cloud computing model is elastic and has scalability, allowing an organization to scale up and down quickly. Its scalability responds to shifting marketing demands without making major investments (Future Processing, 2023). On the other hand, flexibility ensures a more adaptive and agile business model due to its elasticity.

Predictable Costs. Companies using cloud services get advantages from billing cycles monthly (Lim, 2021). This aspect brings about predictability and makes an organization's budgeting easier and straightforward.

Optimized Resource Utilization. These cloud platforms come with automation features and tools that optimize efficient utilization of resources while saving costs.

Lower Maintenance Costs. Migrating to clouds minimizes the burden and costs of physical maintenance and other infrastructures.

Energy Savings . Cloud data centers are energy efficient, lowering utility bills for businesses.

3. Enhanced Data Security and Compliance

Enhanced Security. Cloud providers provide advanced security and encryption protocols that provide vigorous protection against other security threats and data breaches. These providers are better equipped to cater to rising security threats.

Enhanced compliance and security. Clouds have robust security features that simplify the need for compliance with several regulations significant in the current complex regulatory environment. The regulations have constantly updated frameworks, which relieves internal teams from updating and maintaining compliance measures.

Data backup and Redundancy. Cloud platforms operate across various data centers, which automatically backup data, thus ensuring continuity of business in case of a security incident and system failure.

Centralized Security Management. The platform has centralized storage of data, which facilitates the utilization of unified security policies, streamlining security and management protocols. Centralization results in effective and consistent security postures.

Disaster Response . Providers are equipped with resources that easily identify and respond to imminent threats.

4. Increased Flexibility and Collaboration

Global Scalability and Reach . The platform enables companies to scale their operations effortlessly worldwide (Future Processing, 2023). Thus providing it with the agility to contract or expand resources on a demand basis.

Global Accessibility . Cloud solutions enable seamless applications and data access worldwide, empowering global and remote collaborations.

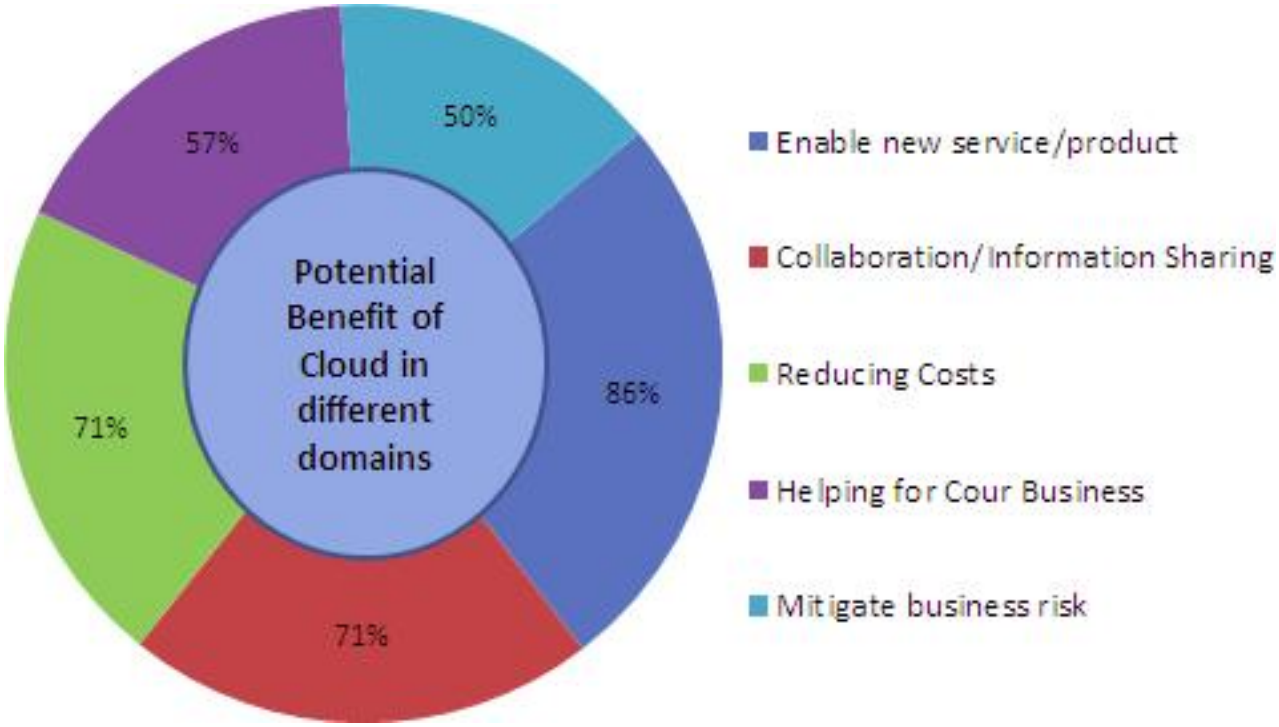

Fig. 1

Simplified Governance and Compliance. Cloud providers provide frameworks and tools that assist businesses in maintaining compliance with several regulatory requirements, thus streamlining the governance process.

Innovation and Competitive Advantage. The platform empowers organizations to deploy new applications and quickly harness advanced technologies like AI, giving them a competitive edge via continuous innovations.

5. Disaster Recovery and Business Continuity

Disaster Recovery. With applications and data being hosted in the cloud, a business is better positioned to quickly recover from unexpected occurrences, which ensures minimal disruptions to its operations.

Geographic Redundancy. The platform allows applications and data to be distributed in various locations in different data centers, which provides additional security for regional disasters.

Recovery time. The platform enhances the process of data recovery. Subsequently, it facilitates prompt restoration of critical information and applicants. As such, an organization gets to resume operations within a short period.

Challenges and Mitigation

Data Security Concerns. This concern arises from relegating confidential information to a third party. Typically, confidentiality needs sturdy security measures. As such, companies should strictly vet the cloud service vendors and establish an appropriate shared responsibility model.

Managing and Controlling Costs . Despite cloud services saving on cost, inadequate/ inefficient budgeting and management may cause unexpected accumulated expenses. Therefore, businesses should continuously monitor their cloud expenses and integrate automated tools that will optimize costs in operations.

Staff Skill Gap . Cloud computing operations require skilled and knowledgeable staff specialized in such operations. The challenge arises if an organization's existing staff do not possess these skills. Thus, an organization should then invest in training or hiring new skilled staff.

Compliance and Regulatory Hurdles . Businesses may experience challenges complying with necessary regulatory measures. Thus, businesses should ensure cloud providers comply with the relevant regulations and laws.

Handling the Complex Migration Process. The process of transitioning is complicated and should be conducted without disrupting business operations. Organizations should plan a detailed plan with expert guidance to ensure a seamless transition.

Cloud Transformation Strategies

Cloud transformation is a fundamental component of digital transformation to revolutionize the online platform. The cloud transformation strategy refers to an organization's approach to migrating into the cloud as seamlessly as possible. Key components of the cloud transformation strategy include;

Rehost ("Lift and Shift")

This migration strategy involves capitalizing on offerings from cloud Infrastructure-as-a-Service (IaaS) to redisposition workloads on the cloud platform. This strategy allows organizations to move an on-premise app to the platform. Accordingly, the businesses shift all applications, workflows and data to the cloud that aligns with their networking, existing storage, and compute requirements without altering the core infrastructure. Configurational and operational constructs are still intact so the rehosting strategy is quick and easy to conduct thus, suitable for businesses lacking in-house cloud-native expertise.

Relocate ("Hypervisor-Level Lift and Shift")

This strategy entails shifting data without affecting the continuing operations, getting new hardware, or rewriting the application source code. As such, an organization can transfer a collection of servers from an on-premise source to the cloud platform. Relocating reduced disruptions and downtime since a client remains connected during migration. This strategy allows companies to have more predictable costs and put restrictions on scalability.

Replatform ("Lift and Reshape")

With this strategy, a business can migrate applications to the cloud while implementing platform development to capitalize on cloud-native capabilities. The app's core architecture and source code remain intact, ensuring legacy operations are operational and ensuring security and cloud-based compliance. This strategy increases agility, flexibility, and workload resilience while sanctioning cloud-native capabilities. It is also cost and time-efficient since an organization does not need to rewrite application code but can still modernize its workload. A business can select its modernization components, which improves its ROI and agility.

Refactor ("Re-architect")

This strategy entails re-architecturing workloads to assist cloud-native competencies from the ground to the top. It needs enormous resources, investments, and an amount of time. Nonetheless, it lets applications support developed capabilities like service computing, distributed load balancing, and autoscaling [2]. Refactoring facilitates monolithic apps' disintegration into microservices to attain higher availability and improve complex automation levels in in-house deployments. Although it is a costly strategy, a well-planned framework costs of operations are reduced compared to legal framework operation.

Repurchase ("Drop and Shop")

This strategy involves changing internal managed systems to available third-party administered services from the cloud vendor. Repurchasing assists groups in retiring legacy systems and shifting to consumption-based SaaS subscriptions modeled to IT costs and generate profits. The services are managed and built by third-party providers; the repurchasing model minimizes operational costs and strives to manage in-house team infrastructure. The option to repurchase simplifies and reduces downtime and improves regulatory governance and scalability. The approach to migration completely capitalizes on cloud-native capabilities, thus mostly used for workloads that need improved user experience and application performance.

Retire

This strategy is applicable when downsizing or terminating apps that are not effective in production. In this case, critical business workloads functioning under ineffective legacy frameworks are retired, which is the start of adopting modernized cloud-native deployments.

Retain ("Revisit")

This strategy is necessary for apps that should continue operating in an existing framework. The workload is then retained if it relies on other applications that need to be transferred [2]. It can also be if no immediate business value is gained from transferring the app to the cloud.

Cloud service model

The main cloud service models are Infrastructure-as-a-Service service model (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS).

SaaS

SaaS is a software distribution and licensing model that has a complete app stack and is provided as a cloud service. An organization's software application and existing infrastructure are hosted on their provider's cloud service and completely maintained and updated by them [13]. The entire computing stack is controlled by the vendors which an organization can access via a web browser. An organization's application operates on the cloud and they can utilize vendor service by obtaining it for free in a limited access or paying license. SaaS does not need downloading or installations in one's underlying computer infrastructure. As such, this aspect eradicates the need for separate installation of applications for each computer used.

The vendor caters to the applications' support and maintenance. It has various benefits that can be leveraged in the cloud transformation [3]. It can be leveraged in cloud transformation since It has minimal cost and eliminates the need for additional hardware and software, thus minimizing implementation and installation costs. Additionally, with SaaS, a business can access the cloud from any location with a device that is internet enabled, thus no physical constraints. It is quickly set up and thus ready to use after a limited time. SaaS has remote and simplified applications, facilitating content transfer, collaboration, and meeting scheduling. Examples of SaaS are Microsoft 365, Google Workspace, ReachOut Suite, infiCE, and Slack. Below is an illustration of some significant SaaS successful businesses;

IaaS

This cloud service model is where the vendor hosts infrastructure constituents that offer storage, computing,

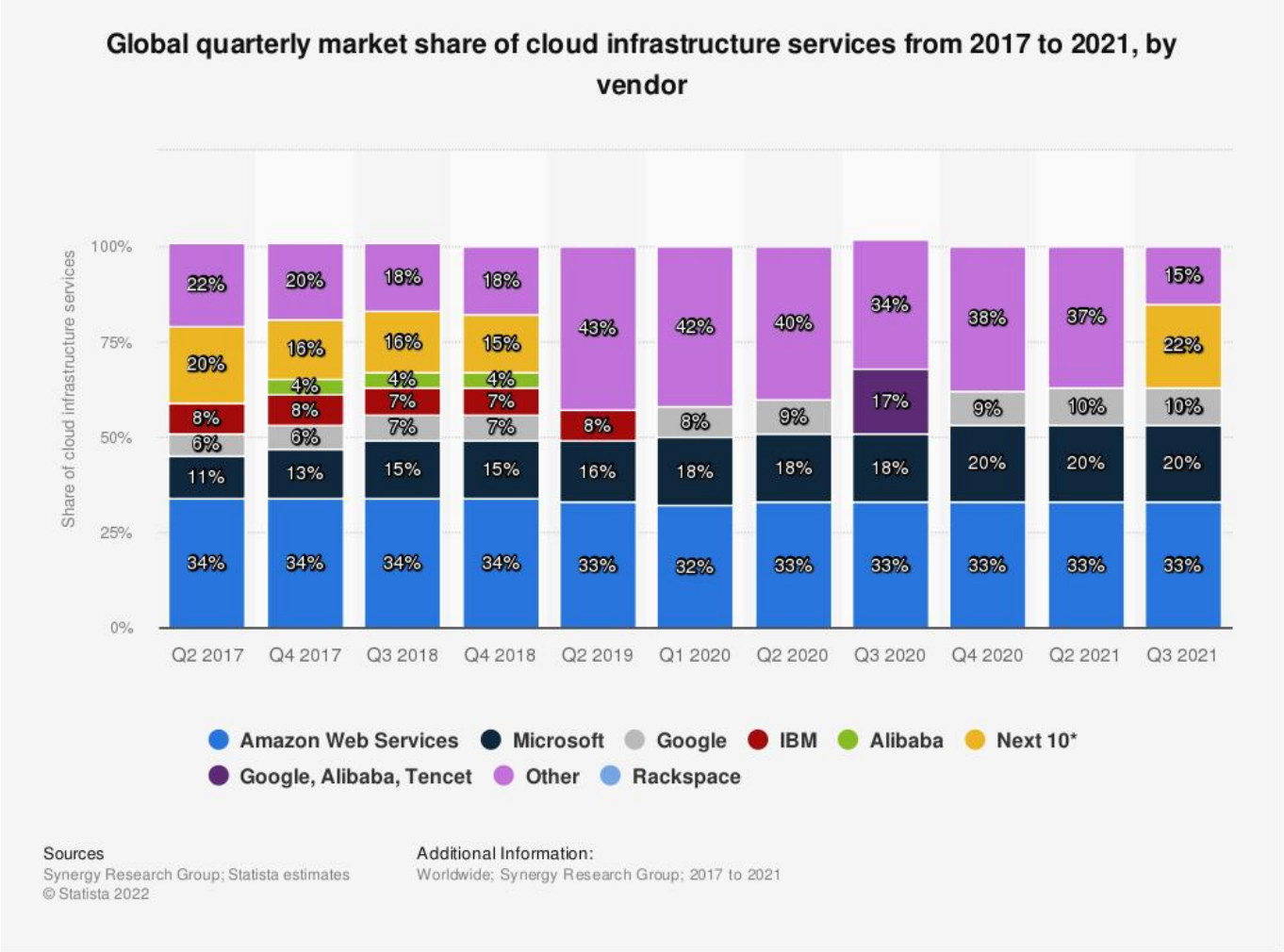

Fig. 2

virtualization capabilities, and networking to a subscriber on a demand basis through the internet [3]. This model eradicates the necessity for organizations to configure, procure, or run infrastructure on their own. They get to pay for what they only use. This model avoids the complexities and costs of maintaining and building physical infrastructure in an on-premises data center. A subscriber only needs to install, manage, and configure software and ensure the data is secure. Examples include Google Compute Engine, Azure IaaS, and AWS EC2.

Its benefits highlight it can be leveraged in a cloud transformation process, they include minimal costs as it eliminates the need for installing costly on-premise hardware. As such, developers can innovate and experiment while saving money and time. It is a flexible cloud model, thus allowing organizations to scale up and down their computing resources swiftly according to their needs. It has quick development cycles, which allows one to spin the required computing infrastructure without waiting for weeks. Therefore, as the most flexible model, it helps organizations customize and manage their IT hardware infrastructure in line with their requirements. It also provides company access to all important computing resources, including networking, storage, and computing, without necessarily buying them.

Platform as a Service (PaaS)

PaaS offers services to users in a scalable and flexible cloud platform to develop, run, deploy, and run apps. It provides the software and hardware resources needed to develop cloud applications [7]. Developers do not need to worry about updating the developing tools and operating system or hardware maintenance [13]. Technically, its platform is delivered via a third-party provider through the cloud. Therefore, businesses purchase pay-as-you-go access to what they need, to develop custom applications, including operating systems, servers, networking middleware, storage, infrastructure, and tools for development.

Furthermore, applications developed in this model environment can be easily deployed, allowing developers to

focus on their application codes. Its benefits include that their providers give developers full access to the complete application development platform they manage and build, giving the developer ample time to deploy and develop. The PaaS developer is in charge of securing the infrastructure and strengthening security. It minimizes downtime, increases business resiliency, speeds recovery, and prevents data loss. Thus, this provider eliminates the need to face the challenges of procuring, running, deploying, and managing infrastructure, thus minimizing operational burden. Thus, it can be leveraged in the migration process.

Security Consideration

Cloud transformation exposes organizations to substantial new risks. The main areas of concern involve data and security protection around data loss prevention, data privacy threats, and breaches of confidentiality.

6. Regulatory and Compliance Requirements

During migration, companies must reassess their compliance and regulatory position concerning the service provider's terms and conditions/policies. This involves verifying data security independently, privacy controls, and compliance to confirm if they attain the relevant standards. Conducting audits is also vital to confirm the validity of the security certifications during and after migration. Proper compliance and regulatory controls minimize risks.

7. Data Exposure

Cloud transformation involves transferring massive data amounts from on-premise systems to the cloud. Security risks become more significant when data is transferred to the cloud. For instance, the application center utilizes several different ranges of ports; cybercriminals are likely to create attacks using multiple vectors to finish their mission. It is also vital to recognize that a company's data may get corrupted by outside forces outside the organization's control [10]. Security attacks may be from service and account hijacking, abuse in using cloud computing, Backdoor Channel attacks, malicious insiders, Cloud malware injection attacks, and Shared technology vulnerabilities. As such, organizations need to ensure their data is encrypted and have the right controls in operations during transit and at rest.

Therefore, there is a need to back up files and configure controls effectively. Once the application is running, there is a need to manage security to prevent and avoid data breaches. Incorporating third-party penetration testing tools helps automate risk management in the cloud infrastructure extensively. Automated web scanning applications can help proactively identify and cater to any vulnerabilities in an organization's application infrastructure in real time.

8. Identity and Access Management

Identity and access management permissions and policies govern who and how data can be accessed. It will depend on the business application target, thus not a one-size-fits-all. Poorly defined Identity and Access Management policies can result in the wrong people accessing confidential data, leading to breaches. There is a need to establish proper Identity and Access Management controls to authenticate user identity at the application level.

9. Control Plane Management

The cloud environment is complex. If one is not prepared, it may be chaotic and challenging. A single misconfigured access control can cause multiple exposures, possibly resulting in security breaches [4]. Configuring a cloud control plane helps avoid such scenarios. It involves a set of controls and settings to orchestrate and manage configurations across an application's baseline. This aspect must be in constant sync with a business data plane to get and process updates in configurations in real life.

10. API Management

Although APIs are a fundamental aspect of cloud transformation, they pose threats to the process of transformation security. Unsecured or unpatched API exposes a company's infrastructure to numerous vulnerabilities. With no efficient services and tools, API management can easily be a significant challenge in cloud transformation.

11. Shared Resources

In the clouding environment, communication is constant between servers between virtual machines. This aspect makes segmentation challenging, given that cloud applications are based on the idea of shared resources. Compromised trust levels and a lack of intra-host traffic visibility may introduce a weak security posture. Below is an illustration of how resources are shared;

12. Process-Oriented Security Configurations

Cloud computing organizations operate in a highly dynamic environment where work is constantly removed and added. Security configurations for workloads may take time, which may create roadblocks. A delay may arise in the usual process to ensure a robust security posture [4]. Therefore, policy shifts need to be approved, identify the appropriate firewalls, and policies updated. Thus, balance needs to be comprehended and updated. If not, discrepancies may arise. As a result, the ri is weakened security posture that can expose important data to risk, which may also cause

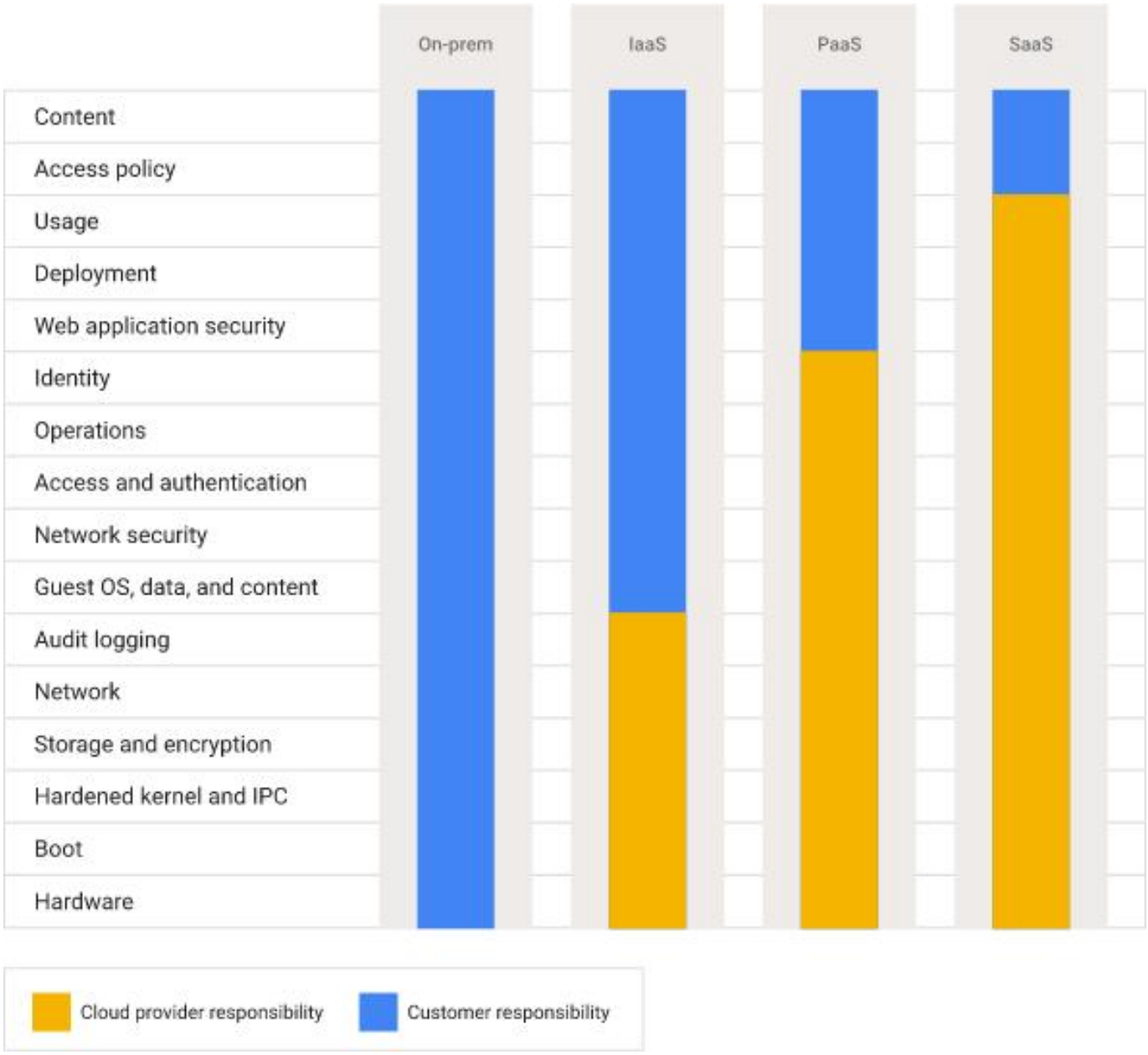

Fig. 3

governance and compliance violations of regulations and policies.

Case Studies

12.1. Spotify: Enabling Extensive Music Streaming

Spotify is a well-known streaming platform. It transferred its architecture into Google Cloud Platform (GCP) to cater to its extensive membership and changing data obligations. Spotify migrated to the cloud to improve its data analytics capabilities, scalability, and reliability. GCP contains robust infrastructure, thus empowering Spotify to access large amounts of data, streamlining its backend operations, and individualizing user experience.

Spotify used a hybrid cloud strategy leveraging various cloud service providers. This migration process was successful as it allowed Spotify to give its millions of users uninterrupted music streaming services while constantly enhancing its content discovery features and recommendation algorithms [5]. They gained a lot of users, as illustrated below;

Spotify encountered various challenges, including difficulties in transferring significant on-premise

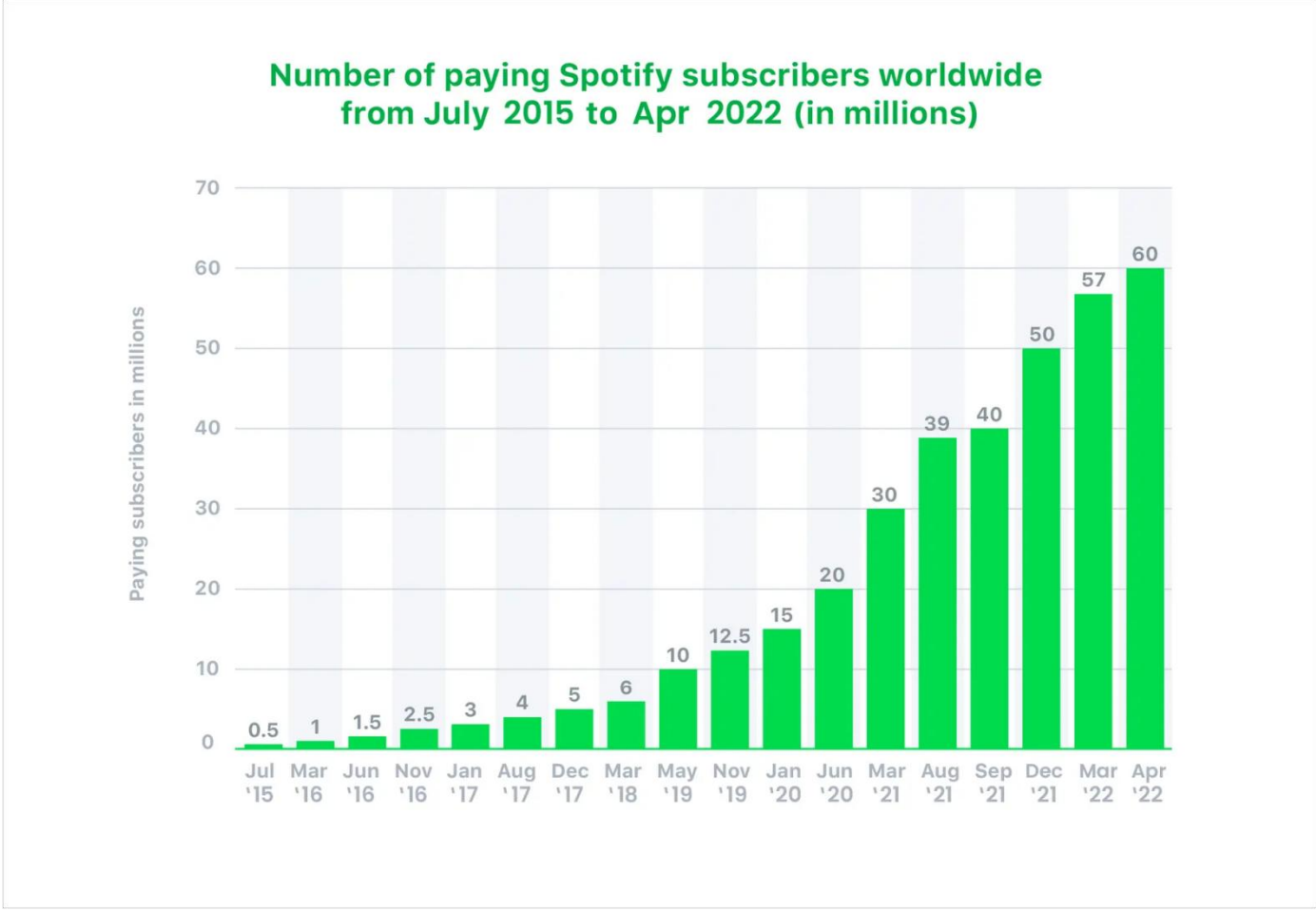

Fig. 4

infrastructure to the cloud with minimal impact on its data integrity and current services.

12.2. Netflix: Scaling for Global Streaming Success

Netflix is a global streaming entertainment service. It decided to embrace cloud transformation to improve the performance of its streaming platform and worldwide scalability. It changed its infrastructure to Amazon Web Services (AWS) from its initial traditional data centers. They used data from their existing systems of users and used it to execute an effective recommendation system.

Embracing the cloud-enabled Netflix to cater to the aggressive growth of its number of streaming as shown below;

The transfer allowed Netflix to capitalize on AWS's substantial infrastructure, allowing quick scaling, enhanced content delivery, and cost optimization [5]. Accordingly, Netflix delivers a seamless experience to the millions of viewers streaming globally. The challenge Netflix experienced at the time was that the migration process was expensive and time-consuming.

12.3. Accelerating NASA's Jet Propulsion Laboratory (JPL Scientific Discoveries

JPL successfully transferred its sizable scientific research series and archives to the cloud. Its cloud provider was Amazon Web Services (AWS) to enhance collaboration, data accessibility, and computational proficiencies. JPL scientists were empowered by cloud migration to analyze and process large data volumes effectively, speeding up their space exploration and scientific study initiatives. By exploiting the scalability of clouds and computing power, JPL gained extensive flexibility, minimized infrastructure expenses, and improved collaborations among researchers working on several missions. The challenge was large data sets with complex simulations from computational demand, which provided a challenge.

Roadmap for Cloud Transformation

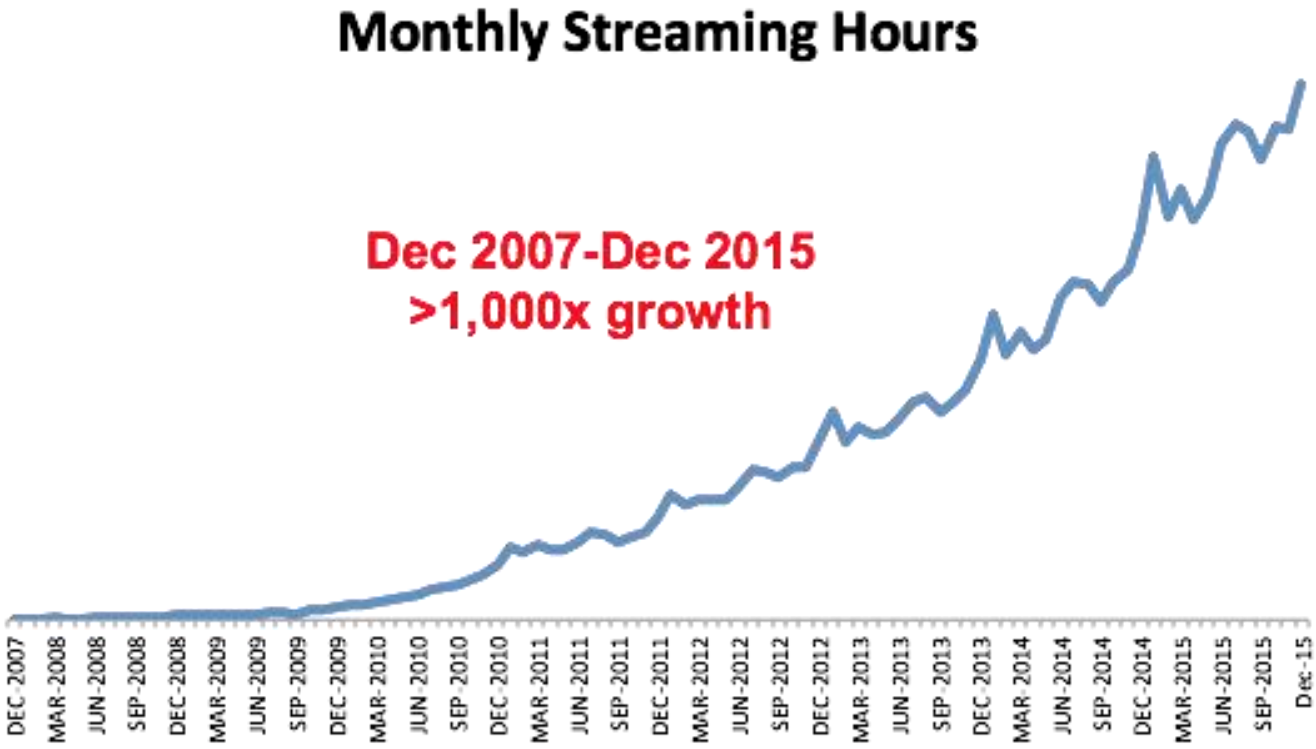

Fig. 5

13. Inspect the Current IT Infrastructure and Assess Cloud-Readiness

Before transitioning to a cloud environment, a company must evaluate its cloud capabilities in its existing hardware and software, data collection, network bandwidth, operating environment, storage requirements, and database compatibility. Accordingly, it analyzes its existing IT landscape, such as data, software, hardware, and integration points. Factors determining how the IT infrastructure will influence cloud migration depend on integration possibilities, scalability, and limitations. The organization should also know the purpose, business process, and usage volume of the applications they plan to mitigate to comprehend whether doing so would be worthwhile [9]. In addition, the business should assess whether existing on-premise applications will work effectively with the cloud if they can easily be modified, and if cloud-native solutions will be required. Then conduct a compatibility analysis to determine which data and application should be moved to the cloud with minimal modifications.

14. Define Objectives for the Cloud Migration Initiative

An organization should understand its value proposition. Assess why the company wants to shift to the cloud, what cloud services they need, and the provider needed to obtain this service. Such questions help in setting objectives [1]. It is essential to understand what a business wants to achieve cloud transformation. A cloud roadmap will be successful depending on objectives that guide it as aligned with overall strategy, its business vision, and IT strategy. Therefore, the company should set SMART goals.

15. Selection of cloud model and Assign Cloud Adoption Owner

A cloud provider can break or make any organization's transformational journey. There are private, public, and hybrid models as available options. Therefore, the company determines the suitable model. Suitability is determined by scalability, compliance, and budget [1]. Other significant parameters include administrative support, upgrades, technology compatibility, and ease of deployment. Furthermore, the model selected should bring stability and longevity to the business.

All organization stakeholders must agree and be ready to

utilize cloud solutions with each of their responsibilities and roles coordinated. It should also decide on persons in charge of cloud operations applications and the operational models used for cloud deployment and updates. Assigning a person who will lead the cloud migration process and ensure that the team knows how to operate functions in the cloud and is responsible for its efficient planning and implementation. If the company lacks a skilled team, they should hire skilled personnel.

16. Establish Cloud Governance and Cloud Security

Cloud governance refers to security rules, regulations, protocols, compliance standards, and procedures put in place and making decisions on how to implement them in the cloud. The business should Conduct a risk assessment to identify and cater to potential risks in security. Before moving to the cloud, an organization should analyze data governance processes and policies. An extensive policy would lay out the process, methods, responsibilities, and how high-risk information can be stored. It should also comprehend rules applied in various data types and applications [9]. Also, determine cloud-specific risks, for instance, cloud architecture vulnerabilities or privacy, and decide upon privacy and access control requirements. Some very efficient security measures in the cloud environment are monitoring of threads, identity access management, encryption, data privacy, and compliance regulation. The business should also conduct an impact analysis to shed light on an organization's gaps in security and comprehend its goals. This analysis will help the organization prepare to respond to any possible challenges.

17. Prepare a Cloud Migration Strategy

Select a cloud strategy that the organization can use for every application. An extensive cloud strategy should cover cloud management workflow best practices, continuity plans, and disaster recovery. A migration plan involves cost analysis, management to estimate the budget, factoring in long-term and immediate costs, and the necessary procedures and tools to track and manage ongoing cloud expenses.

Additionally, change management and training to develop an elaborate communication strategy that accommodates expectations and changes to all stakeholders. Finally, conduct training in the team with the necessary knowledge and skills to equip them [6]. The document should be constantly updated as the cloud mitigation process allows any shifts in cloud services and ensures it is readily available to several stakeholders.

18. Performance Monitoring and Optimization

Establish monitoring tools that will continuously monitor the performance. Conduct regular reviews and optimization to ensure alignment and efficiency to the organization's evolving needs. Optimization and monitoring usage of the cloud will enable a business to leverage the determined efficiencies. The focus could be on metrics that enhance the bottom line and improve user experience. Consistent monitoring will allow early detection of any issues and mitigation of them.

19. Conclusion and Future Trend

Cloud transformation enables organizations to stay agile and competitive in the current digital landscape. Thus, it changes an organization's operations, culture, and technology. Cloud migration benefits are largely categorized under cost efficiency and scalability, enhanced data security and compliance, increased flexibility and collaboration, disaster recovery, and business continuity. Cloud transformation has various strategies: rehost, relocate, replatform, refactor, repurchase, retire, and retain. However, the migration process is prone to challenges including data security concerns, managing and controlling costs, staff skill gaps, compliance and regulatory hurdles, and handling the complex migration process. At the same time, cloud transformation exposes organizations to new substantial risks involving data and security protection regarding data loss, privacy threats, and breach of confidentiality. Reputable cloud providers offer enhanced compliance measures and security to help mitigate risks, enabling organizations to focus on fundamental activities and long-term growth.

As technology continues to evolve, cloud transformation holds interesting prospects. Cloud computing has the infrastructure for ML and AI applications to cater to extensive data. Therefore, ML and AI are driving the future of computing tasks that enable pattern recognition, sophisticated data analysis, and predictive modeling. As ML and AI technologies evolve, the future expects advanced innovative applications across industries.

References

[1] S. Tol, 2021. [Online]. Available: https://www.researchgate.net/publication/348564204_An_approach_to_cloud_transformation_and_cloud_migration/citation/download

[2] S. Sengupta and S. Danan, 2023. [Online]. Available: https://bluexp.netapp.com/blog/aws-cvo-blg- strategies-for-aws-migration-the-new-7th-r-explained

[3] V. Saratchandran, 2023. [Online]. Available: https://www.fingent.com/blog/cloud-service-models-saas-iaas-paas-choose-the-right-one-for-your-business/

[4] This, 2023. [Online]. Available: https://www.torryharris.com/blog/cloud-migration-security-considerations-and-challenges

[5] A. Pathak, 2023. [Online]. Available: https://medium.com/illuminations-mirror/real-life-examples-of-successful-cloud-migration-projects-cloudmigration-2b7ff3451eb3

[6] N. M. Gunturu, "A framework for successful corporate cloud transformation," *International Journal of Computer Trends and Technology*, vol. 70, no. 3, pp. 9–15, 2022.

[7] M. Rosian, R. Brinkhege, I. Gur, A. M. Schleimer, F. V. Scherenberg, and M. Spiekermann, 2021. [Online]. Available: https://www.isst.fraunhofer.de/content/dam/isst-neu/documents/Publikationen/ISST-Berichte/ISST-Report\%20Cloud\%20Transformation.pdf

[8] "Cloud transformation: Benefits and effective strategy. When IT challenges overwhelm your company, I Start Nearshoring," *Future Processing*, 2023.

[9] M. Łach, 2022. [Online]. Available: https://nexocode.com/blog/posts/cloud-migration-roadmap/

[10] H. M. Ahmed, M. H. Ali, L. M. Kadhum, M. F. Zolkipli, and Y. A. Alsariera, "A review of challenges and security risks of cloud computing," *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 9, no. 1-2, pp. 2289–8131, 2017.

[11] K. Chandran, 2022. [Online]. Available: https://hexaware.com/blogs/what-is-cloud-transformation-its-purpose-benefits-and-strategy/

[12] J. Lim, 2009. [Online]. Available: https://www.alation.com/blog/what-is-cloud-transformation/

[13] I. Ashrafa, "An overview of service models of cloud computing," *International Journal of Multidisciplinary and Current Research*, vol. 2, 2014.