ACADEMIC PROJECT

ON

COMPARISON BETWEEN ON-PREMISE AND CLOUD-BASED SOLUTION FOR IT FINANCIAL INSTITUTE

COURSE NAME

ANALYTICAL SOFTWARE AND FRAMEWORKS

DLMBDSA02

SUBMITTED

TO

BY

MR. PARTH LAKHALANI

MATRICULATION NUMBER: 9229810

MASTER OF BUSINESS ADMINISTRATION

COURSE INSTRUCTOR

DR. ANDREW ADJAH SAI

MAY 2024

TABLE OF CONTENTS

1. INTRODUCTION

In this technological era, companies use advanced techniques to efficiently manage large amount of data (Big Data). Companies are aiming to develop new system on platforms such as cloud or on-premise solutions to provide better services and streamline operations. While dealing with big data, companies have to address various concerns like data management, data analysis, and legal compliance. In such a scenario, organizations face challenges in choosing between cloud and on-premise solutions due to deployment, scaling, cost, and security concern (R. Khan, 2023). This study explores cloud-based and on-premises solutions that provide insights that help make right decisions.

1.1 Introduction of on-premise and cloud-based solutions

Organizations used on-premise platforms at the beginning of 1980 because of their reliability and control over data and resources. After the development of new technologies like the internet, cloud platforms have become popular due to their scalability, cost-effectiveness, and ability to provide global access (Taulli Tom, 2020).

1.1.1 On-premise solution

On-premise platforms allow organizations to install and manage their computing resources within their physical locations rather than using cloud-based services. It refers to an infrastructure framework that is completely managed by the company, including hardware and software resources (R. Khan, 2023). On-premise computer solutions allow firms to control and customize computer resources. This framework has served as the foundation for IT companies, allowing organizations to secure their data and more control over infrastructure (Hughes et al., 2021).

In the case of an on-premise solution, organizations have the traditional IT system approach, which involves purchasing and setting up their own hardware and software within their data centres. It offers many benefits, including full control over software infrastructure, which is important for highly regulated businesses with strict security and privacy provisions. In addition, on-premise solution offers more flexibility for customization, enabling organizations to adapt the solution according to unique requirements (Taulli Tom, 2020).

However, there are some important points to consider when using on-premises solutions. This requires having IT professionals to support and manage potential issues that may arise. Additionally, companies must purchase licenses or software to implement on-premises solutions (R. Khan, 2023). The implementation of on-premises solutions comes with major challenges, such as high costs, which often involve large upfront capital expenditures. Additionally, constant maintenance, innovation and research are required. Consequently, this means that the IT department can spend significant time on non-core tasks (Taulli Tom, 2020).

1.1.2 Cloud-based solutions

Cloud-based solution allows organizations to store data on various cloud-based platforms where data can be stored on a centralized computer system. Client, or the user, can access data via the internet to perform operational tasks (Carr, 2024). Cloud computing is the on-demand service model of computing resources like hardware and software with the help of the internet. The main advantage of cloud services is that companies do not need to manage physical servers or infrastructure (*What Is Cloud Computing?*, n.d.-a). In addition, it works on a "pay-as-you-go" model, which means the company will pay for resources that are utilized by itself (*What Are IaaS, PaaS and SaaS?*, 2021). The main difference between cloud and on-premise platforms is that in cloud-based services, users can remotely access the resources offered by third-party providers, which is not possible with on-premise infrastructure, where organizations have to develop their own physical infrastructure. Cloud infrastructure helps companies to save initial investment on infrastructure development (Nandgaonkar & Raut, 2014).

In cloud computing, there are three primary service models: software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS).

1. **Software as a Service (SaaS):** As the term suggests, it has pre-built software infrastructure that provides direct access to online resources for installing, managing, and maintaining different types of software systems.
2. **Platform as a Service (PaaS):** PaaS provides different types of tools and frameworks that help to build, develop, and deploy applications without dealing with the complexities of infrastructure development.
3. **Infrastructure as a Service (IaaS):** IaaS provides virtualized computing resources such as virtual machines, storage, and networking services that organizations can use and pay for as needed.

Table 1.1: Comparison of Cloud Service Models: SaaS, PaaS, and IaaS

Feature	SaaS	PaaS	IaaS
Control	Limited by provider	Application control, infrastructure by provider	Full control over infrastructure
Customization	Limited	Moderate	Extensive
Scalability	Managed by provider	Application scaling	On-demand Scalability
Maintenance	Handled by provider	Infrastructure maintenance	Self-managed with provider support
Examples	Salesforce, Google Workspace	Google App Engine, Azure App Service	AWS EC2, Azure Virtual Machines

Source: Own representation based on (*IaaS, PaaS, SaaS – Cloud Service Model Overview*, n.d.; *What Are IaaS, PaaS and SaaS?*, 2021; *What Is Cloud Computing?*, n.d.-b)

Table 1.1 shows a comparison between three main cloud services. There are some other cloud services like Function as a Service (FaaS), which allows users to manage data or specific functions while the provider handles application management, and Bare Metal as a Service (BMaaS), which provides dedicated server environments similar to the cloud (*IaaS, PaaS, SaaS – Cloud Service Model Overview*, n.d.).

Cloud services come with three deployment models: public, private and hybrid. Public cloud services provide computer resources using internet and various cloud service providers like Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP). On the other hand, private clouds allow organizations to build separate environment on-site or managed by third-party providers. Hybrid clouds combine features of public and private clouds, allowing enterprises to leverage the scalability of public cloud services while maintaining control over critical data and critical operations. (Grover Vikas et al., 2023)

Table 1.2: Comparison of deployment models: Public, Private, and Hybrid Cloud

Feature	Public Cloud	Private Cloud	Hybrid Cloud
Deployment	Shared resources accessible over the internet	Dedicated resources for single organization	Combination of public and private clouds
Control	Provider-managed	Organization-controlled	Shared control between organization and provider
Security	Shared responsibility between provider and users	Organization has full control over security policies	Combination of security measures from both public and private clouds
Scalability	Provider-managed, easily scalable	Scalability depends on infrastructure capacity	Scalability combines resources from both clouds.
Cost	Pay-as-you-go model	Upfront investment, fixed costs	Combination of pay-as-you-go and fixed costs
Examples	AWS, Azure, Google Cloud	VMware, OpenStack	Azure Stack, AWS Outposts

Source: Own representation based on (Chattopadhyay Surajit, 2022; *Choosing a Cloud Management Platform*, n.d.; Grover Vikas et al., 2023)

Table 1.2 compares public, private, and hybrid cloud models. Public clouds provide shared resources and affordable pricing options; private clouds provide dedicated resources with full control over security; and hybrid clouds combine the benefits of both cloud options or cloud with on-premise platforms. The hybrid cloud model integrates public cloud, private cloud, and on-premises infrastructure to create a single flexible and cost-effective IT infrastructure (*What Is Hybrid Cloud?*, 2023). Scalability and control vary among these deployment options.

1.2 Case scenario: IT Financial Institution

For any IT company that deals with a large amount of data and wants to build an efficient platform, choosing between a cloud or on-premise solution is crucial. To make the right decision, the company must consider various factors such as flexibility, scalability, data privacy, data security, and other relevant aspects (Fisher, 2018). To address this issue and analyse both options, the example of an IT company is taken into consideration.

[1]For this study, it is assumed that an IT company is developing a new platform for managing large volumes of sensitive information such as banking transactions, currency exchange, and other financial data. The company aims to develop a new platform capable of handling large amounts of data, also known as big data, and is planning to develop a new platform specifically for data analysis. With the development of a new platform, the company also wants to enhance its security measures against cyber threats and secure sensitive information. The IT institution operates in the financial sector, which has a high-risk environment where it handles a large number of financial transactions across various channels, such as online banking, currency exchange, ATM transactions, and point-of-sale purchases. The main objective of an organization is to deploy an advanced analytics platform capable of real-time fraud detection that effectively manages data privacy regulations. In order to manage and protect its important data assets and defend against cybercrime, the company has to choose between an on-premise or cloud-based solution for its new platform.

1.3 Aim and objective of the study

This study aims to evaluate both on-premise and cloud-based solutions by analysing various factors such as security, scalability, cost-effectiveness, and regulatory requirements. In addition, the article discusses both models and which is most effective for the company's objectives and constraints. As most organizations develop technological platforms for cloud or on-premise solutions, this study examines and evaluates both on-premise and cloud-based approaches by discussing their advantages and disadvantages, taking into consideration various factors such as security, scalability, cost-effectiveness, and regulatory compliance. By discussing both aspects, later this study try to identify the best service model for achieving the organization's objectives and operational requirements by conducting an analysis of both platforms. The ultimate objective of this study is to help with better decision-making, which eventually leads to improved data security and more protection against cyber threats.

[1] **Note:** As per the requirement for this assignment, to discuss various aspects of on-premise and cloud service models, a case scenario is hypothetical (It is not based on a real case scenario) which is based on various resources available in the form of online articles like (*Banking Sector Risk Assessment Report.Pdf*, n.d.; Cutshaw, 2015) and literature available on various platforms, like Google Scholar.

2. ON-PREMISE SOLUTIONS VS CLOUD-BASED SOLUTIONS

This chapter discusses how to implement on-premise and cloud-based solutions for an IT company in the financial sector. It will also discuss advantages, disadvantages, and other considerations associated with both on-premise and cloud computing.

2.1 On-premise solutions

A systematic process, including hardware and software infrastructure management, can implement on-premise services. First, organizations must develop IT infrastructure, which includes purchasing physical components and servers in data centres. It involved the on-site setup of data centres with hardware components like cabling, power supplies, and cooling systems. The next step is the installation of software, which includes the operating system and network configuration (Mattila, 2013). In this scenario, the company deals with a large amount of data that will be generated at regular intervals, which requires additional measures in terms of security and legal compliance.

In the next step, the configuration and customization process begin after the basic hardware software installation, setting up applications with specific business requirements like custom features or integration with internal systems. A separate IT department oversees all this, regularly updating the system and installing security patches, including data backups. In addition, the IT team will monitor security measures like firewalls, encryption, and intrusion detection systems (Mattila, 2013; *SaaS vs On Premise - AWS*, n.d.).

However, there are some other factors, like technical suitability, security, performance, and process management, that need to be considered while implementing on-premise solutions (Mattila, 2013). In this scenario, there are some advantages and limitations to the on-premise service model.

2.1.1 Advantages of on-premise computing

The advantages of an on-premise solution for a financial organization are that it improves data security, regulatory compliance, data privacy, and performance.

1. **Data Security:** On-premise solutions provide better security than cloud-based solutions because data is stored on-site, allowing for more control and security. In addition, local servers provide better security, which makes them less vulnerable to cyberattacks (Fisher, 2018). In this scenario, an on-premise solution offers better security when an organization handles sensitive information such as baking transactions and other financial data.
2. **Regulatory compliance:** Highly regulated sectors, like the financial sector, must adhere to strict regulatory compliance requirements such as data privacy, data security, and other legal considerations. On-premise services allow organizations to match regulatory compliance (Fisher, 2018). For a given case scenario in which the organization is working in a specific region, it must follow regional and other IT regulations, and an on-premise solution provides more flexibility for regulatory compliance.

3. **Data privacy and control:** For an on-premise platform, the organization has full control over its data resources (R. Khan, 2023). In this scenario, financial institutions handle sensitive data, which provides full control over their infrastructure, enabling them to implement more precise security measures and ensure compliance with data privacy rules and regulations (Summers, 2020).
4. **Performance:** On-premise services have their own internal network for accessing data, which improves performance by increasing efficiency and reducing processing time (Summers, 2020). In this scenario, operations like data analysis or data management will be faster than those in the cloud, which requires high-bandwidth internet.

2.1.2 Disadvantages of on-premise computing

There are several limitations related to on-premise solutions, including capital intensiveness, scalability constraints, maintenance exigencies, geographic expansion limitations, and vulnerability to single points of failure.

1. **Limited Scalability:** On-premise systems face several scalability issues, requiring the company to increase its hardware resources, which can lead to additional costs. In addition, if a company wants to upgrade its system, it also requires new hardware components. This process is complex and time-consuming (Nandgaonkar & Raut, 2014). In this case, companies working in the financial sector have to regularly upgrade their systems because of security concerns; an on-premise approach might not be suitable.
2. **Cost:** For on-premise computing, the upfront cost of computational resources includes hardware, software, electricity, and rental costs (R. Khan, 2023). In the case of financial institutions, companies have to invest a high number of resources, which might not be suitable for small start-ups or organizations.
3. **IT team:** On-premise solutions increase the burden on IT teams because of regular monitoring, maintenance, and updates. Such an operation required skilled IT professionals, which comes with additional costs (R. Khan, 2023; *SaaS vs On Premise - AWS*, n.d.). In this scenario, the organization may not benefit from this process, as the need for skilled employees can pose an additional burden.
4. **Remote access issue:** With an on-premise platform, remote access is a major concern, leading IT companies to promote remote work due to its various benefits. When remote workers connect to on-site servers via the internet, poor connectivity or other technical issues might affect overall productivity (*SaaS vs On Premise - AWS*, n.d.). In the given scenario, financial institutions may face difficulty working remotely.

There are other limitations to on-premise solutions, time-consuming deployment, maintenance, risk of data loss, disaster recovery and compliance costs. (*SaaS vs On Premise - AWS*, n.d.)

2.2 Cloud-based solutions

To implement a cloud-based solution, organizations first have to identify the most suitable cloud service provider that provides the best services to the company at the lowest cost. To select the best cloud service, organizations need to analyse the features and services offered by different cloud service providers, like Amazon web service (AWS), Google cloud platforms (GCP), Microsoft Azure etc. After that, organizations set up formal infrastructure and services on the cloud platform, including virtual servers and storage (Tomar et al., 2023).

When implementing the cloud approach for a scenario involving sensitive data, the company must consider several important factors. The most sensitive is security; therefore, encryption, authentication, and isolation of data should be implemented to keep sensitive data secure (Hoener, 2013). In a given scenario, organizations want to analyse a large volume of data. In such cases, cloud services, which provide the best tools for data analytics, are a second important consideration. Many cloud service providers (CSPs) offer advanced platforms for data analysis, such as AWS. These platforms include tools such as Athena, Amazon EMR, and Redshift, which are equipped with the latest technology support for machine learning (ML) and predictive analysis (*Data Lakes and Analytics on AWS*, n.d.).

Furthermore, there are some other factors that play a critical role in selecting the right cloud partner. Factors like customization, support, backup, scalability, accessibility. Customization ensures that a cloud service provides for specific business needs. Support ensures that services are provided in accordance with the SLA (service level agreement) requirements. Backup hosts potentially have unlimited data storage capacity with different pricing options. Accessibility makes it easier for users to reach the services with an internet connection (*Data Lakes and Analytics on AWS*, n.d.).

2.2.1 Advantages of cloud computing

A cloud computing solution comes with various advantages, like data management and security. Cloud computing ensures scalability, cost efficiency, global accessibility, security, and compliance.

1. **Scalability:** The cloud platform has greater scalability, allowing an IT company to easily scale up and down its services based on demand at the lowest cost. This is very helpful for managing large amounts of data during periods of high demand (R. Khan, 2023). If a company grows in the given scenario, cloud computing will be the best option due to its scalability, which allows organizations to effectively manage resources with minimal cost.
2. **Cost efficiency:** Without any initial investment in infrastructure, the organization is able to allocate additional services or storage when needed (Fisher, 2018). In the given scenario, if new companies or start-ups want to launch financial services, the cloud service will provide essential services without requiring any initial investment.

3. **Global accessibility:** Cloud computing allows an organization to easily run its businesses internationally without having to build physical infrastructure in each location (*SaaS vs On Premise - AWS*, n.d.). For a given scenario, if an organization offers financial services globally, the cloud platform provides multiple instances at different locations by offering data centres and allowing anyone to access resources via the Internet at any location.
4. **Advance security:** Cloud service providers come with advanced security measures such as encryption, authentication, and threat detection. These security measures can help improve a company's ability to protect valuable data from cyberattacks (*Cloud Security (AWS)*, n.d.). In a scenario where a company handles sensitive data from the financial sector, implementing advanced security measures can enhance security.
5. **Compliance support:** Most cloud service providers help with compliance; for example, Amazon Web Services (AWS) supports 143 security standards and regulatory compliance certifications, including PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171, which support compliance requirements globally (*Cloud Compliance (AWS)*, n.d.). For any organization providing international services, such compliance support is crucial.

2.2.2 Disadvantages of cloud computing

However, adopting a cloud computing solution comes with some limitations, such as data privacy, dependency, security threats, and regulatory compliance.

1. **Data breaches:** One limitation of the cloud platform is the increased risk of data breaches, which put personal information at risk and create significant legal issues related to customer protection (Kolevski et al., 2021). The company handles financial transactions, such as banking transactions. Such data breaches pose a high risk for organization.
2. **Cloud Service Dependency:** When a company relies on cloud services, it typically encounters a dependency issue if the cloud service provider fails. Due to a service failure, a company may experience problems with performance and data accessibility. If a company works in finance, it needs continuous access to sensitive data. In this scenario, the failure of cloud services could result in a significant delay, and the company might face financial losses (Gagnaire et al., 2012).
3. **Potential security risks:** A cloud service provider offers world-class security measures, although it is vulnerable to cyber threats, security breaches, and unauthorized access (Shi et al., 2010). In such cases, the company needs to put in additional skills and resources to protect data and threats from cyberattacks.
4. **Regulatory challenges:** Despite the compliance support provided by cloud service providers, companies still face challenges in dealing with complex regulatory compliance. Organizations must stay informed about the latest regulations and make sure their cloud deployments follow updates. In such cases, the company should regularly update penal privacy rules to global standards to avoid regulatory fines (Saini et al., 2022).

2.3 On-premise vs cloud computing

To simplify the basic concept, the previous section discussed how to implement both platforms in a given scenario, along with the advantages and limitations of both approaches. In the given scenario, the organization operates in a highly sensitive sector, such as finance, and deals with a large amount of data. The organization must decide which approach is most suitable for their services. In this section, both platforms will be further compared and analysed to determine the best platform for a case. The decision-making process will be based on four key factors: flexibility and scalability, cost analysis, data control and security, compliance, and regulatory requirements.

2.3.1 Flexibility and scalability

On-premise solutions offer more flexibility in terms of infrastructure; companies have full control over their infrastructure because they manage and configure all hardware and software resources on-site (R. Khan, 2023). However, one of the major issues is scalability. If an organization grows, it requires additional hardware resources, which is time-consuming and costly. On the other hand, cloud solutions do not offer greater flexibility in terms of infrastructure because all resources are controlled by cloud service providers. When it comes to scalability, companies can easily adjust their resources based on demand without making any upfront investments (Summers, 2020).

2.3.2 Cost analysis

On-premise solutions initially require a significant capital investment in hardware and infrastructure and require regular maintenance and security upgrades. Cloud-based solutions come with a pay-as-you-go model that offers better scalability at more affordable rates, allowing the company to easily scale up or down services according to demand without making a significant upfront investment, which makes cloud-based solutions more economical (Grover Vikas et al., 2023).

2.3.3 Data control and security

On-premise solutions provide better security than cloud-based solutions because data is stored on-site, allowing for more control and security (Fisher, 2018). This is especially crucial for financial institutions handling sensitive information, enabling precise security measures, and ensuring compliance with data privacy rules (Summers, 2020). However, on-premise solutions can be costly and require significant maintenance. Cloud service providers, on the other hand, come with advanced security measures such as encryption, authentication, and threat detection (*Cloud Security (AWS)*, n.d.). However, cloud-based approach increased risk of data breaches, which can lead to significant issues (Kolevski et al., 2021).

2.3.4 Compliance and regulatory considerations

On-premise solutions allow organizations to easily comply with regulatory compliance, providing flexibility for regional and specific IT regulations (Fisher, 2018). However, it will not be effective if the service is expanded to multiple regions, and it also requires additional investment for

expansion. On the other side, cloud service providers, such as AWS, support a variety of compliance standards and certifications that are critical for international services. Still, companies face challenges in keeping up with complex regulatory requirements (*Cloud Compliance (AWS)*, n.d.; Saini et al., 2022). While on-premise solutions offer more control, cloud solutions provide extensive compliance support internationally. A balanced approach might involve using a hybrid solution to leverage both benefits.

3. DECISION MAKING PROCESS FOR CASE SCENARIO

In the given case scenario of an IT financial company, both on-premise and cloud-based solutions come with several advantages and limitations when considering all four criteria. From the previous discussion, on-premise solutions provide more flexibility in terms of infrastructure control, but they come with significant investment. In addition, on-premise platforms face scalability issues; they are limited due to maintenance and additional costs for hardware components. For the given scenario, in terms of flexibility and scalability, a cloud-based solution provides an edge to companies that might grow and want to expand globally. Cloud-based solution is a better option in terms of scalability and cost efficiency. As it works on a pay-as-you-go model, it is more suitable for growing businesses without any significant investment. However, the cloud-service model has some challenges in terms of data security and privacy due to its dependency on cloud service providers. Another issue with cloud platforms is regulatory and compliance requirements, which are critical for any financial institute. However, while cloud service providers support compliance, organizations must update new regulatory requirements.

Table 3.1: Decision making between cloud and on-remise solution

Sr. No.	Factor/Criteria	On-Premise	Cloud based Solution	Decision Making
1	**Flexibility and Scalability**	High control, low scalability	High scalability, limited control	Cloud (Hybrid)
2	**Cost Analysis**	High upfront and maintenance costs	Cost-efficient, pay-as-you-go model	Cloud (Public)
3	**Data Control and Security**	High control, better security	Advanced security, potential risks	On-Premise for critical data
4	**Compliance and Regulatory**	High customization for compliance	Extensive compliance support, ongoing updates	Hybrid

Source: Own representation based on discussion.

Table 3.1 shows a comparative analysis between cloud and on-premise solutions. The analysis indicates that out of four different factors that help in the decision-making process, flexibility and scalability favor the cloud-based solution due to its high scalability with minimal investment in infrastructure. However, organizations operating in highly regulated sectors like finance cannot ignore factors such as data security and privacy. In such cases, on-premise services offer better security. Finally, when it comes to compliance and other regulatory requirements, both platforms have unique advantages: the cloud provides extensive compliance support globally, while on-premise offers high customization options. Overall, out of the four factors, two support a hybrid approach, while cost favors the cloud-based platform and data security favors on-premise services.

3.1 Hybrid cloud for IT Financial Institution

Companies can store sensitive information and critical application data on-premise using hybrid cloud storage to maintain optimal control with high security. For data processing and analysis, a cloud platform is a more suitable option due to its scalability. This setup helps organizations enhance security measures against cyber threats by using advanced security tools for encryption and threat detection. All sensitive data remains in the on-premise data centre. By combining both services, a hybrid model is more suitable for the company's objective of developing a platform with high security capabilities and advanced analytical tools.

Table 3.2 Service distribution between on-premise and cloud platform for Hybrid cloud

No.	Factor	On-Premise (Reason)	Cloud (Reason)
1	Flexibility and Scalability	Sensitive operations (full control, better customization)	Data analytics and high-demand tasks (scalability, resource availability)
2	Cost Analysis	Critical infrastructure (high upfront investment justified)	Non-critical operations (cost-efficient, pay-as-you-go model)
3	Data Control and Security	Sensitive data (better security, control over data)	General data processing (advanced security measures, efficient management)
4	Regulatory Compliance	Local regulations (high customization for compliance)	Global compliance (extensive support from cloud providers)

Source: own representation based on discussion

Table 3.2 shows the service distribution between on-premise and cloud-based platforms, with four key factors. On-premise solutions manage sensitive operations that require more control and customization for flexibility and scalability, while cloud platforms handle data analytics and tasks with high scalability. On-premises can be used for critical infrastructure, and the cloud can be used for other operations, which will be more economical. For data security, an on-premise platform is used to store sensitive data, such as bank or ATM transactions; on the other hand, a cloud can be used for general data, such as backups or non-sensitive data. On-premise platforms offer high customization for regulatory compliance, while cloud platforms support global compliance.

3.2 Limitation of Hybrid cloud

Despite all the advantages, there are some limitations with hybrid clouds. Hybrid clouds are complex to manage due to the integration of different platforms, which requires advanced skills and resources. The most critical aspect is data management between two platforms to avoid operational disruptions. Additionally, it requires regular security updates and compliance monitoring during data transfer between on-premise and cloud systems (Grover Vikas et al., 2023; S. U. Khan & Ullah, 2016).

4. CONCLUSION

This study compares both on-premise and cloud-based approaches for financial institutions that deal with large volumes of data. To analyse both approaches, this study considers a hypothetical scenario where an IT company wants to build an effective data management and analytics system. The objective of the study is to compare and analyse the flexibility, scalability, cost, data control, security, and compliance aspects of both solutions.

Implementing on-premise solutions involves setting up data centres and managing infrastructure, which includes hardware and software resources. The on-premise platform comes with several advantages, like data security, data privacy, regulatory compliance, and performance. However, there are some limitations, which include scalability, high cost, resource management, and remote access issues. Organizations that work in sensitive sectors like finance will benefit from security, privacy, and performance. However, high costs, limited scalability, and resource management may not be suitable for the company.

A cloud-based solution allows organizations to store data on a centralized system provided by a cloud service provider where users can access information using the internet. The main advantage of cloud-based services is that organizations do not have to manage physical infrastructure. In addition, it works on a “pay-as-you-go” model, which helps minimize the cost of services used by companies. Cloud model comes with three main service models: software, or SaaS (pre-built software infrastructure), platform, or PaaS (inbuilt tools for application development), and infrastructure, or IaaS (virtualization of computer resources). There are three main deployment models: public, private, and hybrid. Each of these service and deployment models comes with a variety of features, like control, security, scalability, and cost efficiency. For a given scenario, there are several advantages, including scalability in resources, cost efficiency, global accessibility, and advanced security features with regulatory compliance support. However, there are several issues with the cloud service model, which include data breaches, dependency on cloud service providers, security, and limited regulatory support. When selecting a cloud service provider, there are also some other factors to consider, like customization, support, backup, and scalability.

While comparing both platforms, the on-premise solution offers more infrastructure flexibility because the company manages all hardware and software resources on-site. However, scalability poses a significant challenge as it necessitates additional hardware, resulting in additional costs and time. On the other hand, service providers fully manage cloud-based solutions, enabling scalability without any initial investment, whereas on-premise systems require ongoing maintenance and capital investment for expansion. Another advantage of cloud platforms is cost efficiency because of the pay-as-you-go model. On-premises offers control over data and security, which is crucial for organizations in the given scenario. The cloud also provides advanced security measures, but it is vulnerable to cyber threats. Both platforms offer compliance support; on-

premise services offer local support, while cloud services offer international support. Both platforms come with unique advantages; in a given scenario, security, compliance, and scalability are crucial, which leads to a hybrid solution.

For the given scenario, the hybrid cloud model provides a balanced approach by combining the strengths of on-premise and cloud solutions. It ensures flexibility, scalability, cost-efficiency, and enhanced security. It uses an on-premise platform for data security, management, and control, as well as a cloud for data scalability and analytical operations. However, it comes with operational complexity; to manage critical operations, it requires advanced skills and resources.

In conclusion, the hybrid cloud approach effectively works by combining both on-premise and cloud platforms, ensuring flexibility, scalability, cost-efficiency, and data security with compliance. It helps organizations achieve their objectives with data management, security, and analytics.

5. BIBLIOGRAPHY

Banking Sector Risk Assessment Report.pdf. (n.d.). Retrieved May 21, 2024, from https://www.resbank.co.za/content/dam/sarb/publications/media-releases/2022/pa-assessment-reports/Banking%20Sector%20Risk%20Assessment%20Report.pdf

Carr, N. (2024, May 16). *Cloud computing | Security, Cost Savings & Flexibility | Britannica*. https://www.britannica.com/technology/cloud-computing

Chattopadhyay Surajit. (2022). 10.5.5 Public, Private, Hybrid, and Community Clouds. In *Nanogrids and Picogrids and Their Integration with Electric Vehicles* (edsknv.kt0130GMD1). Knovel. https://app.knovel.com/hotlink/pdf/rcid:kpNPTIEV03/id:kt0130GMD1/nanogrids-picogrids-their/public-private-hybrid?kpromoter=federation

Choosing a Cloud Management Platform. (n.d.). Intel. Retrieved May 23, 2024, from https://www.intel.com/content/www/us/en/cloud-computing/cloud-management-platforms.html

Cloud Compliance (AWS). (n.d.). Amazon Web Services, Inc. Retrieved May 24, 2024, from https://aws.amazon.com/compliance/

Cloud Security (AWS). (n.d.). Amazon Web Services, Inc. Retrieved May 24, 2024, from https://aws.amazon.com/security/

Cutshaw, J. (2015). *Online authentication challenges for financial institutions in a complex digital era* [PhD Thesis, Utica College]. https://search.proquest.com/openview/f3c44fa3059a0e9f093887ec1e8a0ec9/1?pq-origsite=gscholar&cbl=18750

Data Lakes and Analytics on AWS. (n.d.). Amazon Web Services, Inc. Retrieved May 24, 2024, from https://aws.amazon.com/big-data/datalakes-and-analytics/

Fisher, C. (2018). Cloud versus On-Premise Computing. *American Journal of Industrial and Business Management*, *8*(9), Article 9. https://doi.org/10.4236/ajibm.2018.89133

Gagnaire, M., Diaz, F., Coti, C., Cerin, C., Shiozaki, K., Xu, Y., Delort, P., Smets, J.-P., Le Lous, J., & Lubiarz, S. (2012). Downtime statistics of current cloud solutions. *International Working Group on Cloud Computing Resiliency, Tech. Rep*, *1*(30), 136.

Grover Vikas, Verma Ishu, & Rajagopalan Praveen. (2023). Achieving Digital Transformation Using Hybrid Cloud—Design Standardized Next-Generation Applications for Any Infrastructure. In *Achieving Digital Transformation Using Hybrid Cloud—Design Standardized Next-Generation Applications for Any Infrastructure* (edsknv.kt013GY2S1). Knovel. https://app.knovel.com/hotlink/pdf/rcid:kpADTUHCD2/id:kt013GY2S1/achieving-digital-transformation/finding-right-balance?kpromoter=federation

Hoener, P. M. (2013, June 11). *Cloud Computing Security Requirements and Solutions: A Systematic Literature Review* [Info:eu-repo/semantics/bachelorThesis]. University of Twente. https://essay.utwente.nl/69114/

Hughes, L., Sweeney, D., & Kasunic, M. (2021). Planning and Design Considerations for On-Premises Computing Environments. *2021*, 1–2.

IaaS, PaaS, SaaS – Cloud Service Model Overview. (n.d.). Intel. Retrieved May 23, 2024, from https://www.intel.com/content/www/us/en/cloud-computing/as-a-service.html

Khan, R. (2023). *On-Premise or Cloud (The not so obvious choice).* (edsbig.A756645179; Vol. 39, Issues 154–155). Gale Business: Insights. https://search.ebscohost.com/login.aspx?direct=true&db=edsbig&AN=edsbig.A756645179&site=eds-live

Khan, S. U., & Ullah, N. (2016). Challenges in the adoption of hybrid cloud: An exploratory study using systematic literature review. *The Journal of Engineering*, *2016*(5), 107–118. https://doi.org/10.1049/joe.2016.0089

Kolevski, D., Michael, K., Abbas, R., & Freeman, M. (2021). Cloud Data Breach Disclosures: The Consumer and their Personally Identifiable Information (PII)? *2021 IEEE Conference on Norbert Wiener in the 21st Century (21CW)*, 1–9. https://doi.org/10.1109/21CW48944.2021.9532579

Mattila, T. (2013). Comparing preconditions for cloud and on-premises development. *Cloud-Based Software Engineering*, 1–8.

Nandgaonkar, S. V., & Raut, A. B. (2014). A comprehensive study on cloud computing. *International Journal of Computer Science and Mobile Computing*, *3*(4), 733–738.

SaaS vs On Premise—AWS. (n.d.). Amazon Web Services, Inc. Retrieved May 23, 2024, from https://aws.amazon.com/compare/the-difference-between-saas-and-on-premises/

Saini, J. S., Saini, D. K., Gupta, P., Lamba, C. S., & Rao, G. M. (2022). [Retracted] Cloud Computing: Legal Issues and Provision. *Security and Communication Networks*, *2022*, e2288961. https://doi.org/10.1155/2022/2288961

Shi, A., Xia, Y., & Zhan, H. (2010). Applying cloud computing in financial service industry. *2010 International Conference on Intelligent Control and Information Processing*, 579–583. https://doi.org/10.1109/ICICIP.2010.5564162

Summers, L. (2020, September 17). *On-Premise, Cloud, or Both? Four Considerations to Build Your Strategy*. Oxford Global Resources. https://www.oxfordcorp.com/on-premise-cloud-or-both-what-you-should-know-before-deciding/

Taulli Tom. (2020). 2.1 On-Premise vs. The Cloud. In *Robotic Process Automation Handbook—A Guide to Implementing RPA Systems* (pp. 28–30). Apress, an imprint of Springer Nature.

Tomar, A., Kumar, R. R., & Gupta, I. (2023). Decision making for cloud service selection: A novel and hybrid MCDM approach. *Cluster Computing: The Journal of Networks, Software Tools and Applications*, *26*(6), 3869-3869–3887. Springer Nature Journals. https://doi.org/10.1007/s10586-022-03793-y

What Are IaaS, PaaS and SaaS? | *IBM*. (2021, October 20). https://www.ibm.com/topics/iaas-paas-saas

What is Cloud Computing? (n.d.-a). Google Cloud. Retrieved May 21, 2024, from https://cloud.google.com/learn/what-is-cloud-computing

What Is Cloud Computing? | *Microsoft Azure*. (n.d.-b). Retrieved May 23, 2024, from https://azure.microsoft.com/en-in/resources/cloud-computing-dictionary/what-is-cloud-computing

What Is Hybrid Cloud? | *IBM*. (2023, June 5). https://www.ibm.com/topics/hybrid-cloud