jamk

Main Factors Influencing Companies to Advocate for On-Premises Systems in the Era of Cloud Technology Dominance

Puwakgahawela Muhandiramlage Anushka Nisansala

Master of Engineering, Degree Programme in Cyber Security YTC24S1
May 2025

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Puwakgahawela Muhandiramlage Anushka Nisansala

Main Factors Influencing Companies Advocate for On-Premises Systems in the Era of Cloud Technology Dominance

Jyväskylä: Jamk University of Applied Sciences, May 2025, 96 pages

Master of Engineering, Degree Programme in Cyber Security YTC24S1. Master's thesis.

Permission for open access publication: Yes

Language of publication: English

Abstract

Skafi, Yunis and Zekri (2017) exemplified the increased usage of cloud computing adoption in organizations worldwide which highlighted the significance of examining the aspects that might have impact on the adoption of this computing paradigm in companies operating in different industries and sectors. Younus et al (2024) illustrated that the cloud is a more popular aromatic buzzword in the IT world which had revolutionized the approach for company's businesses. It was well agreed upon by the researchers that cloud computing service models have significant effect on achieving cost efficiency and better payoffs and return on investments in information technologies and systems. However, this computing model is still relatively recent and represents a low fraction of the total Information Technology (IT) invested, even if it is growing at a faster pace compared to traditional computing models (Skafi, Yunis and Zekri, 2017).

The main aim of the study was to conduct a theoretical and a practical study on the factors effect on the decision of adopting on premise computing by the IT organizations in Sri Lanka. Moreover, the study provided a comparative analysis of the factors for On-Premises and Cloud computing thus the respective effect of each factor on the decision for on premise computing. Moreover, this provided practical recommendations were proposed to address and mitigate the impact of the most influential factor driving the preference for on-premises IT systems in Sri Lanka IT companies.

With the usage of 73 sample participants from the IT companies in Western province of Sri Lanka, primary data was collected. A qualitative plus a quantitative analysis were performed as per the data analysis. Results as per the correlation analysis, security, performance governance/compliance depicted a positive relationship with decision for on-premises computing where cost, scalability and downtime/high availability showed a negative relationship with decision for on-premises computing. Statistical analysis was confirmed, 'security' factor as the most influential factor on the decision on on-premises computing. Recommending that IT companies can undertake the right cloud architecture, adhere to the robust security controls while maintaining compliance with industry-specific regulations, such IT companies can adapt cloud computing with greater degree of security.

Keywords/tags (subjects)

On-Premises computing, Cloud Computing, IT companies, Main factors, Azure

Miscellaneous (Confidential information)

-

Contents

Figures

Tables

List of Abbreviations

GUI - Graphical User Interface

GCP – Google Cloud Platform

GSP – Government Security Program

HIPAA- Health Insurance Portability and Accountability Act

VLAN - Virtual Local Area Networks

TCO - Total Cost of Ownership

CAPEX – Capital Expenditures

FERPA- Family Educational Rights and Privacy Act

SLA - Service Level Agreement

SME – Small and Medium Enterprises

AWS - Amazon Web Services

IT – Information Technology

NIST - National Institute of Standards and Technology

CSA - Cloud Security Alliance

API – Application Programming Interface

CSPM - Cloud Security Posture Management

SSE - Storage Service Encryption

TLS - Transport Layer Security

RBAC - Role-Based Access Control

SIEM - Security Information and Event Management

GCP - Google Cloud Platform

SOAR - Security Orchestration, Automation and Response (SOAR)

DPU - Data Processing Units

VM – virtual Machines

IoT – Internet of Things

ETL – Extract, Transform, Load

BI – Business Intelligence

KYOK - Keep Your Own Key

BYOK - Bring Your Own Key

DEK - Data Encryption Keys

CSP - Cloud Service Provider

HSM - Hardware Security Modules

IAM – Identify and Access Management

HSM – Hardware Security Module

VPN – Virtual Private Network

1 Introduction

1.1 Background of Study

"Choosing the right infrastructure is a strategic decision that will impact your organization for years. Take time to evaluate options, consult with experts, and weigh the trade-offs." Mathias Golombek (2025), CTO, veteran in the data industry.

Overall, the IT industry and cloud-related technologies encompass many components and offer ease of use and maintenance through cloud service providers. These providers leverage IT experts worldwide to help organizations design infrastructure tailored to their web service requirements (Kumar et al., 2019). Therefore, organizations are increasingly shifting to cloud solutions instead of investing heavily in on-premise infrastructure. Traditional setups require ongoing maintenance costs and involve greater risks. In contrast, the cloud has transformed the IT industry by offering organizations a more efficient and low-risk alternative allowing them to create a complete infrastructure with just a few clicks, tailored to their specific needs (Younus et al., 2024). Similar to DevOps practices, organizations can define their infrastructure as code using configuration files and build that infrastructure with tools like Terraform, an open-source utility (Laghari et al., 2018).

As stated by Younus et al. (2024), cloud computing has become a prominent buzzword in the IT industry, revolutionizing how companies conduct their business. It facilitates information sharing, collaboration, and the administration of computing and web resources. With the rise of the internet, cloud computing has redefined how businesses operate, enabling companies to move beyond traditional on-premise IT infrastructure. Globally, most cloud service providers offer similar core services. In Asia, major players such as AWS, Azure, and Google Cloud Platform (GCP) dominate the market. This rapid exchange and promotion of cloud-based services suggests strong and ongoing growth, with no significant decline expected in the near future (Walters, 2012; Nazir et al., 2020).

Choosing the most suitable cloud service provider can be challenging for organizations due to the presence of multiple competitors in the market, each offering varying web services and pricing models. The top three providers AWS, Azure, and Google Cloud Platform (GCP) dominate the

industry by delivering high-quality services, though they tend to be more expensive compared to other alternatives (Shaikh, 2019, 2022). Azure, a product of Microsoft, is the second most popular cloud service provider; however, its graphical user interface (GUI) is often considered less user-friendly compared to AWS (Mishra et al., 2022a). Meanwhile, Google Cloud Platform (GCP), the third major provider, is rapidly increasing its market share and continuously introduces new web services in response to evolving market demands. In addition to the major providers, other cloud service providers such as Alibaba Cloud, Rackspace, and Huawei Cloud are also actively competing in the market (Kunz et al., 2022). Organizations typically select a provider based on factors such as cost-effectiveness, availability of comprehensive documentation, and strong customer support especially when assistance is needed for configuration or troubleshooting issues (Ghosh et al., 2014). For optimal service delivery, it is essential to examine the characteristics and relationships among the leading cloud providers Google Cloud Platform (GCP), Microsoft Azure, and Amazon Web Services (AWS). Their service offerings begin with competitive value propositions, and each provider's long-term commitments indicate the strategic direction they may pursue. Key factors to consider include the range of current web services offered, pricing models, and any customer incentives or discounts (Whaiduzzaman et al., 2014; Chou, 2015).

According to Skafi, Yunis, and Zekri (2017), the growing adoption of cloud computing across organizations worldwide underscores the importance of examining the factors that influence its adoption. This is particularly relevant for companies in various industries and sectors, including the IT sector. Researchers widely agree that cloud computing service models have a significant impact on achieving cost efficiency, as well as improving payoffs and return on investments in information technologies and systems. However, despite its rapid growth, this computing model remains relatively recent and still represents a small fraction of total IT investment, though it is expanding more quickly than traditional computing models (Skafi, Yunis, and Zekri, 2017). The goal of this research is to conduct both a theoretical and practical study on the factors influencing the decision to adopt either on-premise computing or cloud computing in IT organizations. Additionally, this study will provide a comparative analysis of the factors and their effects in both on-premise and cloud computing, specifically focusing on Azure. The study will also offer practical recommendations

for choosing the ideal computing system whether on-premise or cloud based on these factors and their respective impacts.

1.2 Problem Statement

As far as corporate use is concerned, cloud computing has become more suitable. The cloud computing services such as Infrastructure as a Service and other models enabled with providing many solutions for the prevailing problems rather conventional on-premise computing systems(Coop, 2014). Capital investment requirement, slow service delivery of the IT hardware as per the slow rate of procurement process, lack of agility are some of the main problems identified. Further, as an IT professional with more than ten years work experience in the field, the researcher has observed, many IT companies in Sri Lanka still favor traditional on premise IT systems over cloud-based solutions, even though cloud technology dominates the industry. As to explore this, the researchers' aim is to uncover the reasons behind this practice, whether this practice involve security concerns, cost, control, or client preferences etc. Therefore, the problem statement of this study is to investigate, What are the main factors driving IT organizations to prefer on-premise IT systems over cloud-based solutions?

1.3 Research Questions of the Study

1) What are the main factors driving organizations to prefer on-premise IT systems over cloud-based solutions in Sri Lanka IT companies? (Theory part -> IT Infrastructure Decision Making)

2) How to perform a comparison of Cloud computing system and On-Premises system for each identified factors Sri Lanka IT companies? (Theory part -> Comparison of Cloud computing system and On-Premises system)

3) What recommendations can be proposed to address and mitigate the impact of the most influential factor driving the preference for on-premise IT systems in Sri Lanka IT companies? (Theory part -> Cloud computing , On-Premises system)

1.4 Objectives of the Study

1) Identifying the main factors which effect on making the decision of On Premise Computing or Cloud Computing in IT organizations.

2) Executing a comprehensive comparison on identified factor in relation to On Premise Computing and Cloud Computing in IT organizations.

3) Provide recommendations to correctly address and mitigate the impact of the most influential factor for the preference of On Premise Computing To determine the most influential factor driving the preference for on premise IT systems.

1.5 Scope of the study

The scope of this thesis focuses on understanding the factors influencing IT decision-makers' preference for on-premises IT systems over cloud-based solutions, despite the growing dominance of cloud technology. The study aims to explore the decision-making processes within organizations by analyzing the main factors that weigh heavily on the choice between on-premises and cloud IT infrastructure. Meanwhile examine the organizational benefits and detriments associated with on premise approach with its deployment. Furthermore it is essential to study how 'decision-makers in IT' organizations evaluate the trade-offs between cloud and on-premises systems.

With the practical and theoretical knowledge, it is essential to identify the main factors influencing for the final decision thus assessing the weight of main factors with the most influential factor plus the least influential factor that drive the IT organizations to undertake on premise or cloud computing models.

This research study will propose recommendations, which are practical to mitigate the impact of the most influential factor contributing to the preference for on premise or cloud computing systems.

1.6 Puropse of the study

The study's purpose is to provide a deep analysis of the factors affecting for the decision of undertaking on premise computing model or cloud computing model in IT companies, as well as provide a deep insight on the behavior of each factor in relation to these two models while providing recommendations to reasonably address and mitigate the impact of the most influential factor for the aforesaid models(Tachu, 2022). The research findings would be really value for IT leaders when taking decisions on cloud computing and on-premise computing in their respective IT organizations. The decision on cloud computing or on-premise computing adaptation in the present IT world is a matter of growing cyber threats, rapidity of globalization, big data, increasing risk, legal requirements, information governance evolution (Collins, 2014; Lee et al., 2017; Ruiter & Warnier, 2011). As per an exploration of concurrent practices in the state and enterprise environments, managers and the leaders of IT organizations can utilize the valuable findings of this research study.

1.7 Practical use in the study

As per the success chance irrespective of the computing model which has undertaken, appropriate management of the aspects in relation to identified factors from the research study and their respective magnitudes on cloud or on premise computing models, will be certainly directing the organizations plus the IT project managers efficiently and effecctively for the attainment of organizational goals. In addition, concerning on the factors and the practical recommendations which are proposed will furnish the upgrading proposition of these two models of on-premise computing and cloud computing (Correia and Martens,2022). Meantime, challenges in any project i.e. risk mitigation, cost reduction etc. in relation to cloud computing or on-premise computing, this research effort's findings will be really supportive as far as those types of decision makers are concerned.

1.8 Limitations of the Study

The main limitation on this research study is concerning only a limited number of IT organizations in Sri Lanka though the on premise and cloud computing models are acknowledged worldwide. In

addition, most of the MNC level IT companies are not represented in this research study. According to Lovelock and Anderson (2019) plus Goasduff (2019), under consideration of various stages and cloud adaptation priorities globally as far as the data gathering is concerned, a very serious issue. The global context may not be accurately represented subsequently(Olufowote, 2017). Moreover, the second limitation of this research study is, the research study is concerning only Microsoft Azure as the cloud computing service. The other cloud computing services are not concerned for this research study. This research study is not going to tap the technical implementation details of hardware or software systems on both on premise and cloud computing models.

Sabol et al. (2013) illustrated new challenges could be introduced with the usage of previously validated study because of the dynamic movement of IT industry, its practices and definitions, its business strategies and concepts etc. Meanwhile, this research study is concerning only a small set of factors affecting for the decision of undertaking the on premise computing or cloud computing. There are other factors which are not considered for this research study but affecting for the above decision making process.

1.9 Chapter Organization of the Study

The thesis of this research study will be comprising of mainly nine chapters, references list along with the appendix section. The nine main chapters will be, Introduction, 3 chapters for Literature Review, Methodology, Data Analysis followed by Conclusion, Policy Implications and Recommendations. Chapter 1 which is Introduction is comprising of all the related background Information, Problem Statement, Research Questions and Objectives, Scope, Purpose, Significance of the Research Study, Limitations etc. Literature Review which is Chapter 2,3 and 4 are comprising of all the previous scholarly works all around the world which can strongly back the theoretical background in relation to the research study.

Chapter 5(Methodology) will be comprising of all the definitions of all the pertaining variables to the research study from world-wide accepted research scholars, operationalization, conceptual framework, hypothesis etc. The Data Analysis chapter(Chapter 6) will include a comprehensive primary and secondary data analysis connected to the research study. The Chapter 7,8,9 which are

Results, Conclusion and Recommendations will come up with all the valuable conclusions from this research effort plus the recommendations and policy implications the researcher is suggesting by based on the research results derived.

2 Main Factors for selecting an architecture

As far as cloud computing and its adoption by the organizations are concerned, more research has been carried out by scholars over the years. According to Tyagi (2015), cloud computing system is a platform of providing services on demand and computer resources which centralizes system related resources through a distributed architecture. Kushwaha (2020) elaborated, via internet, the cloud computing system inter-connects databases, applications, storages and servers. Accordingly, Skafi, Yunis and Zekri (2017) concluded that, for successful cloud computing system adoption, organizations should have technical readiness. A comprehensive understanding and assessment of risks, benefits plus processes of cloud computing must be there before the decision to undertake cloud computing system by the organizations (Avram, 2014). As far as the SMEs perspective of adoption of cloud services, it's very important to consider the support from the topmost people of the SME, size of the organization, previous experience etc. (Alshamaila and Papagiannidis(2013). In several countries, for different rates of cloud adoption, IT friendliness significantly impacts (Abolfazli, 2015). Further illustrated, low cost of ownership, elastic scalability, low capital investment, low level of complexity, high availability are the unique features of cloud computing over on-premises computing. According to Google Executive Plus Internet Guru Vince Cerf (Hugos & Hulitzky, 2011), cloud computing is substantially larger scale and flexible compared to the previous computing utility.

Amazon Web Services (AWS) which was introduced by Amazon in 2006, is an elastic cloud computing. The concept was there in different forms well before that. Permitting people to use the internet more and more, Mukherjee (2019) introduced the advantages and the ideal suitability of AWS cloud to the community. As per the research, it proved the cost cutting for the organizations with the use of cloud as the organizations pay only for the services used hence those services are high in efficiency and quality. High-performance processing, data centric encryption, regulatory compliance,

tractability, security, least cost, quantifiability, data storage etc. are the advantages of AWS cloud computing service.

In 2008, the 'Beta' phase of Google search engine launched as a result of its updating. 'Oracle Cloud' was launched by Oracle in 2012 as a result of its cloud computing initiative. As per Uzoma and Okhuoya (2022), cloud computing is all about, without any influx of a personal computer installation, IT infrastructure accessing via a computer network.

NIST provided the most acceted and widely used definition for cloud computing. "Paradigm for providing universal, convenient, on-demand network access to a shared pool of configurable computing resources i.e.networks, servers, storage, applications, and services". According to Rozsnyai et al. (2011), with a minimal service provider interactions and management effort, it can be controlled. Acoording to Mel and Grance(2011), minimal effort of the management and sevice provider interaction, cloud computing serve as a pool of resources with on-request, convienient network access. From one data centre to the other, delivering of excess capacity is high in scale, volume and speed (Hugos and Hulitzky, 2011). Chou (2015) elaborated, as far as provision of information technology and resources to organizations are concerned, the emergence of cloud computing is a development(Chou, 2015). Allowing to respond promptly to the dynamics of information technology related business needs plus better leverage of information technology related investment by the organizations, cloud computing assists a great deal (Lindner, 2010; Marston et al., 2011). Business dynamism related rapid adoption of the cloud computing as of its scalability and flexibility, it a prominent thing to emphazise. The investment for research and development plus on the innovative core business activities by an organization is very easy with efficient information technology is taken place (SATW,2012). According to Nielsen(2013), processing, sharing memorey, software and other IT services on demand, network capacity of remote computers can be leveraged via internet by the cloud computin systems. To deal with any IT undertaking at anytime from any place, work and system developments, plans executions etc, the innovative technology of cloud computing can be made use (Skafi, Yunis and Zekri,2017). The five pivotal attributes of cloud services aaccording to Cloud Security Alliance Report(2009) are: 1)

Resource pooling, 2) broad network access, 3) Measured service, 4) On-demand self service and 5) Rapid elasticity.

Nielsen(2013) characterized five main attributes of cloud computing. Lian et al.(2015) identified unique characteristics of cloud computing which can be utilized to leverage on the technology by the decision makers.

1) High Performance : Higher capability of data analysis, higher data storage capacity, higher power of computing.

2) Flexibility and dynamic scalability : According to the business volume, distribution or re-distribution of IT resources can be performed automatically.

3) Low-Cost : Resources utility (hardware and software) is efficient where cost can be lowered.

4) Ubiquitius : Physical location or the device they use are not problems. Through the network, systems can be accessed by the users.

5) Reliability and easy maintenance : As per a better maintenance and security, professional teams are placed in cloud computing.

As far as the dynamic organizations are concerned, flexible, cost effective and saclable IT products are offered by cloud computing. For long-run success and for a smooth transition, cloud computing can be implemented by considering vital factors such as cost management, security, adoption strategies, infrastructure, compliance, technical implementation etc. Pyke(2009) finely expressed how it is a paradigm shift from the traditional computing paradigm to cloud computing.

Nucleus(2009) examined allocation of market-oriented asset resource along with cloud infrastructere and delivery models. Fox(2009) studied risks associated with the migration process from legacy systems to cloud plus cloud architecture real-world opportunities and implementation challanges. Compared to on-premise server installations, many research work have been carried out by the scholars on management, significance, influencing factors, application of cloud

computing as of its wide-spread within the organizations. According to Dempsey and Kelliher (2009) illustrated, with the usage of ransomeware, how hackers have intensified their activities and destroyed the security of the cloud computing systems through which stolen the valuble data by damaging the data storages. This bolds the necessity of higher-security level to face the cyber attacks and ensure the security plus protection of infrastructure, data, applications etc. Since hackers strategically organize and execute their activities, organizations with cloud computing systems must spend reasonable time and effort for malware detection and safeguard data. The security experts to improve the supreriority of the security and response time, the hackers continuous attacks really helped(Baladini et al., 2017). As of the resistance from the cyber attacks and protecting sensitive data, cloud computing systems using organizations must recruit highly skilled and talented security experts for their respective organizations. While barriering unauthorized access to critical information, this type of highly skilled and talented IT security experts play a highly pivotal role in mitigating risks, monitoring and detecting security breeches as to ensure smooth and un-interupted functionality of organizations. Al-Sharafi et al (2017) elaborated most noteworthy ten factors which affect for the decision of cloud computing adoptation by the decision makers. IT readyness, perceived security and privacy, compatibility, top management's support, complexity, governament support, relative advantage, cost effectiveness, competition and trust are such factors. In accordance with Injadat et al (2021), the most prominet challenges of cloud computing adoption and widespread are cost effectiveness, trust and security. Misra and Mondal (2011) concluded that 71% of orgnizations believe cloud computing is a real technology option. 70% is agreed on cloud computings' ability to make the business flexible. Prompt market responsing ability carries 62%. Stay focus on the core business secured 65%.

I. On Premise Computing compared to Cloud Computing

According to Skilton (2010), there are some on-premise and cloud computing systems differentiating characteristics. It is depicted with the usage of below table.

Table 1: Difference between On Premise Computing and Cloud Computing

Considered Factor	On Premise Computing	Cloud Computing
Hosting Location	Management of hardware is performed within the ornization's premise.	Hosting software/harware out of the organization's premise. Or private cloud service within the organization's premise.
Resource Provisioning	Based on the demand's peak, software and hardware are provisioned.	In accordance with the actual demand, provisioned the services. It ensures a well-managed service.
Demand Management & Monitoring	As a measurement of present SLA performance and demand usage forecasts, utilizing service management monitoring.	As per the obtainment of savings from cost against oning and provisioning of assets, short run 'burst' demand is focused by the services
Cost & Billing Model	Payments and usages are regulated with the usage of compensations and chargebacks.	As per the virtual assets optimization, made use of statistical automated scaling.
Scalability & Capability Management	Unpredicted fluctuations in demand can lead to overprovisioning or underprovisioning.	The provider/seller of cloud service is taking such risks.

Ownership & Investment Methodology	Assets ownership is vested with the organization as the investor.	Assets ownership is vested with the provider/seller. With the increment of shared resources users, the providers are expecting economies of scale.
IT Management & Operations	Management and operations are done by the investor.	User of the service is muted from IT infrastructure and operations. SaaS is below the cloud.

(Source: Skilton, 2010)

The study(Kelton, 2009), commissioned by Avande (2025), as of the arrival of new technology options, a world-wide IT consultancy related giant ended up with an imperative duration of time within the technology industry. Accordingly, many IT staff personnels reported, due to the lack of security and control over data, they prefer on-premise computing over cloud computing. Meantime, responses from the majority of staff stated, expenses are really high as far as the prevailing on-premise computing systems are concerned. Nevertheless, prompt responses to the market, higher rate of agility and reduction in initial IT cost led more investments on cloud computing by the early adopters.

As per the organizations strugle with the change plus productivity increment of few resources are concerned, with the intention of minimizing cost, technologies were explored more than 50% of the organizations. The ultimate aim of this effort is to save money. 71% of global decision makers in relation to IT industry provided their consent for cloud computing. The Usa(80%) and global (65%) IT related executives trust the reduction of initial cost by the cloud computing systems. On-premise computing is very expensive according to the four fifth majority of respondants. 61% of globally operating organizations are still not the users of cloud computing systems while some are their as

early adopters to the system. No any integration plan by the 80% of users of on-premise computing with cloudcomputing as far as one year of future time is concerned.

" The benefits and the reasonable positive difference offered by cloud computing is keep on understanding thoroughly by the IT related decision makers globally. The only hidering factors of such computing system are control and security. There is an essentiality in the industry to adequately tap this type of hiders and develop a long term strategy to gear-up the cloud computing services plus make use of it's business value capitalizatio process" said by Tyson Hartman (2009) the Avanade Global Chief technology Officer. Privacy and security are decisive in the decision of computer systems adoptation(Avram,2013). Further illustrated, in the process of data privacy protection efforts, various requirements arise for the organizations thus there is a doubt of adequate enough of data security in cloud computing.

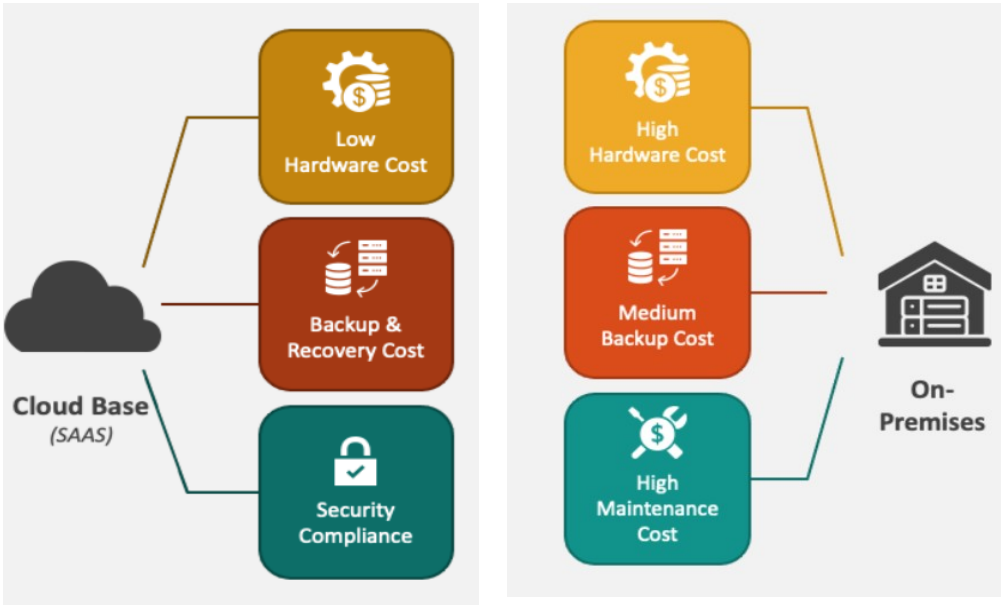

Figure 1 : Some costs pertaining to Cloud and On-Premise Computing

Source: Collidu.com (2024)

II. Some costs affiliated with Cloud Computing

Software development or acquisition costs: Software development and acquisition costs are significant factors in cloud computing agreements, as they determine how businesses access and

utilize cloud-based applications. Cloud agreements typically cover three primary software models: internally developed software, externally purchased software, and cloud-native applications that grant users access to cloud resources.

Infrastructure purchase cost: The infrastructure purchase cost is a significant investment for cloud service providers, as it involves acquiring the essential hardware and technology required to build and maintain cloud computing environments. These costs include expenditures on storage systems, mainframe equipment, servers, networking components, and data centers, all of which form the backbone of cloud services. By allowing customers to access via internet, the cloud service provider is possessing the location for infrastructure in public clouds.

III. Some of the Cloud Computing operations

Following operations(not limited to) are considered as main operations which are offered by a cloud computing system. 1) Content management, 2) System-wide reporting, 3) Accounting services, 4) Electronic mail, 5) Human Resources Management, 6) Security, 7) On-Line market place etc.

IV. Cloud offering Business Benefits

Social media, internet, email etc. are popular cloud technologies deploy in the organizations according to the CircleID (2009) survey. Threats of security and loss of control reasonably impact on such technologies adoptation by the organizations. As far as computing systems in organizations are concerned, a new paradigm is represented from the cloud computing. By based on the survey results, facts which back the business value of cloud systems are as follows:

- Cloud systems facilitate organizations on flexibility improvement(70%), prompt response to the market dynamism(62%), core business focus(65%), latest technology usage approach(51%).
- Once the real benefits of cloud systems have been revealed, organizations have more tendency towards accumilating more cloud services(organizations usage of cloud systems is one-third).
- Respondants plus organizations acknowledge minimized initial cost in cloud systems.

According to Hartman(2009), as to be globally competitive, new technologies adoptation along with best practices continuation for an organization is a must hense future aspect of evolusion of IT might be cloud computing. Skafi, Yunis and Zekri (2017) stated that as it's in-built scale-up or down capability according to the customers requirement, cloud computing offers customers to issue finance only for utilized computing resources which are served by the cloud service provider on the demad made by the customer. Further, it increases day to day operations effectiveness of the organization in a cost efficient manner as no need of purchasing hardware, software by the organizations thus offering adequate storage, bandwith, operations, electricity as per the requirement.

V. Challenges to face when implementing Cloud Computing System

Benefits and challenges are inevitable in new technology. According to Isom and Holley (2012), though the vital factor is security, initial deployments offer good experience for service providers thus starting to fade as organizations which are an initial stage barrier. Further, assets security must be analyzed and weighed under a cloud strategy by the organizations, and it needs to identify the issues to be addressed by the organization in advance of cloud's total embracement. Data protection, integrity and unauthorized access risk are the main challenges in cloud computing system implementation hence the term 'security' is highly correlated with the aforesaid challenges. As far as Groom and Jones (2018) illustration is concerned, increased availability of information to the applications which are totally outside to the cloud through this integration surrounding, from the governance level of information, a unique access privileges set must be preserved and noticed. Getting assured on the cloud service provider's ability to meet security compliance requirements is a responsibility of the receiving company. The problems won't move one place to another through the process of reviewing prevailing applications efficiency. Control of machines which are virtual through management, scaling and provisioning can be done with the usage of cloud orchestration. With the improved management of cloud, it is possible for cloud apps to move data sets used by cloud(Raj, 2014).

VI. On-premises or Cloud Decision (How to make it?)

Organizational unique wants and priorities will shape the choice for cloud or on-premises infrastructure. Yen (2023) summarized key feature areas against measures of each solution. Accordingly,

- Infrastructure

  Infrastructure is owned and controlled by IT teams in on-premises but there is a limitation for them. Cloud service providers own major control over cloud infrastructure where a great deal of infrastructure is invested by the service providers to ensure faster response, greater uptimes and resources etc.

- Budgeting

  Resources which are under-utilized are a waste of money though there is a fixed price in on-premises. Capacity upscaling costs additional finance where long-run cost effectiveness will be possible as far as on-premises is concerned. In cloud computing, a portion of payment can be done only for the server utilization portion hence shutting it down after the business task completion is also possible. Therefore cloud computing system is more economical.

- Implementation

  Considerable amount of comprehensive planning, purchase of hardware and procurement, proper installation and configuration is required in on-premise infrastructure. In cloud computing system implementation, selection of a proper cloud service provider, data migration, application migration, resources configuration are must. Normally, cloud service providers offer comprehensive support, tools plus documentation for a smooth migration from on-premise system to a cloud system which are best industry practices over the years. Optimal performance and ensure minimum burden is a responsibility of the organization which is executing the cloud migration process.

- Security

Security is well-managed and everything is under control within the own devices as far as on-premise system is concerned. Tailor-made firewalls, intrusion detection and security protocols can also be implemented within the on-premise system. When it comes to the cloud computing system, the service provider maintain compliance regulations and industry standards through deploying specialized security teams where service providers investment is very high in threat detection systems, data encryption and access controls.

- Compliance

  As far as compliance and regulatory requirements are concerned, on-premise allows organizations to have total control over it. As to ensure certain compliance standards are met, organizations can use monitoring and customized security controls. Confirmation of security standards and industry-specific regulations are met, attestations and compliance certifications are offered by the cloud service providers. Organizations which are handling sensitive data and highly regulated industries really value that approach of cloud service providers.

- Data Accessibility

  Teams which are geographically apart and remote, the accessibility barriers comes to the arena in on-premise computing systems. Cloud computing systems are allowing remote and geographically separated teams to work collaboratively and effectively via internet. Users are facilitated to access data by being in any location (universal accessibility) in a convenient and flexible manner.

- Deployment

  Except for hardware based infrastructure, cloud system and on-premise system share almost same procedure as far as software deployment is concerned. If there is any necessity of an additional server in the data center, order, rack, network and provision it is done.

- Management

Hardware maintenance (drives replacement, maintenance of such drives and hardware, network maintenance, configurations management, power handling, buildings construction and maintenance) is a must in on-premise system. Many of the maintenance and management tasks are done by the cloud service providers. Users have to perform only making few adjustments trough software tools or management dashboard.

In essence, most of the previous scholarly efforts (Kalra and Moukhtar, 2024; Skilton, 2010; Collidu,2024,) identified a common base of factors, namely cost, security, performance, scalability, downtime, reliability, infrastructure requirement, implementation, data accessibility in relation to a decision making of cloud or on premise computing. More and more organizations are impacted on the process of making the correct decision either to undertake cloud or on-premise computing systems (Yen, 2023). Fisher (2018) provides a comprehensive comparison of cloud computing system against on-premise computing system.

As this aforesaid research of Fisher(2018) illustrates costs in relation to both the cloud and on-premise systems, it is pivotal for this research study. For any organization, the research provides implications which are very important plus impacting in long-run when the organizations are in the virtie of taking the decision to undertake either cloud system or on-premise system. The real-time financial side of the cloud computing system is thoroughly discussed within the research effort.

A deep insight on the technical part of the cloud computing and on-premise computing systems is equiped in Fisher's work apart from the cost analysis. Control, security, customization abilities, security etc. are main topics under which each computing system is analyzed with advantages and disadvantages. As far as an organization is concerned, thses aspects are very vital. Besides, innovative capacity, adaptability and agility of an organization is affected through cloud computing (Microsoft Azure) and on-premise computing adoptation is deeply discussed in the Fisher's paper. As far as concurrent market dynamism is concerned, thses aspects are very much significant for present organizations.

Skafi, Yunis and Zekri (2017) elaborated, it needs to further study the factors which make it possible the digital technologies adoptation where there are proven doubts in transfering sytems and data to cloud. This is further compounded by the fact that there is a lack of literature providing sufficient insight into the general factors that influence the adoption of cloud computing by the organizations or adoption of on premise computing. Step forward to reasonably tap the prevailling niche, cost, security, performance, scalability, downtime/high avaialbility, compliance/governance factors are provided deeper insights through this research study.

3 Comparison of 2 architectures for each identified factor

3.1 Microsoft Azure Architecture

Microsoft's Azure is an open and flexible cloud platform that enables users to quickly build, deploy, and manage applications across a global network of Microsoft-managed datacenters, offering both infrastructure and application services, or "Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) capabilities" with "built-in data services, advanced analytics, and rapid development service development tools" all running in Microsoft's global network of Microsoft-managed datacenters (Microsoft, 2015). It can be used for a lot of different use cases from simple file servers or network / storage appliances to more complex solutions such as mobile and web services, IoT, and hybrid cloud-based deployments. Azure is also supported by open-source technologies and can be utilized in on-premises, or as a completely cloud-based technology. It provides modular cloud services to enable new business solutions that lower costs, reduce risk and provide the freedom to develop and manage data applications. What makes Azure different is that Azure provides a secure and consistent cloud service platform for any workload unlike other cloud service providers, Azure is the only hybrid cloud offering that has a sophisticated, built-in security and management service that works across multiple Microsoft and non-Microsoft environments. Azure is part of the Microsoft Trusted Cloud, which is known for its best-in-class security, compliance, privacy, and reliability, and is supported by one of the largest, most vibrant ecosystems of partners and a network of people (Microsoft, 2025).

3.1.1 Cost

One of the biggest drivers of when it makes sense for an organization to go on-premises or cloud is really cost. A significant advantage of using cloud computing is the offloading of capital and operational costs from the user to concerns who are invested in deploying and maintaining computing infrastructure. These responsibilities are pushed to cloud service providers and the enterprises free up more time to concentrate on their core business operations. Microsoft Azure

enables this transition with a broad array of cost management resources to support organizations in the efficient management and optimization of their cloud costs.

I. Introduction to Cost Management in Azure

Microsoft Cost Management is a family of FinOps (Financial Operations) capabilities which empower organizations to track, analyse, and manage spending on Microsoft Cloud services. These tools are available to people with appropriate permissions to billing accounts, subscriptions (including specific subscriptions), resource groups, or management groups. Cost Management is available in the Azure billing and resource management interface, and it's also in its own tool specifically designed for FinOps teams managing cost across larger footprints. By incorporating these capabilities within internal financial workflows, companies can improve visibility and accountability across departments, facilitating the faster realization of cost-efficiency targets.

II. Core Functionalities

The Microsoft Cost Management efficiently provide a set of functionalities that enhance businesses to monitor and analyse their expenditures, urge their budget controls, and optimize well resource allocation. Organizations are able to:

- Create reports related to the cost within the Azure portal or Microsoft 365 admin centre.
- Leverage Power BI for sophisticated dashboard creation and to generate correlation between data.
- Establish proactive cost monitoring through budgets, anomaly detection, and alerts.
- Configure shared costs across departments or projects using tagging and allocation rules.

- Export cost information to external systems for broader financial analysis.

III. Reporting and Analytics Tools

Different reporting tools for Cost Management in Azure:

- Cost Analysis
- Power BI Integration
- Exports and the Cost Details API
- Connectors for Azure

Microsoft Cost Management offers several robust reporting and analytic capabilities that the cloud financial customer needs in order to understand cloud spend. Cost Analysis delivers fast, on-the-fly cost search for instant insights and integrates with Power BI to build rich dashboards and in-depth reports. Additionally, Cost Details APIs and exports provide the flexibility for organizations to include cost data into external systems and automate financial processes. In the case of multi-cloud enterprises, Azure connectors help users to consolidate and track their spending across Azure and AWS at one location for better cost governance and analysis.

IV. Budgets and Alerts

Azure budgets provide the ability to drive financial accountability through threshold alerts across a plan or a set of plans using actual or forecasted cost. Budgets can be linked to the organisational objectives and reviewed on a routine basis (e.g.: monthly, quarterly, annually). Budgets automatically reset at the end of a given time period (except when specified otherwise). Notifications can be setup to notify stakeholders of spending that nears or crosses the set thresholds to keep costs at the acceptable range.

V. Automation Capabilities

Microsoft provides multiple automation options to streamline cost tracking and reporting, which are:

- Cost Details APIs
- Pricing APIs
- Budgets and Alerts APIs:
- Invoicing APIs
- Reservation APIs

Microsoft Azure provides a rock-solid suite of automation facilities to make the cost tracking and reporting life easier. Through granular APIs, such as the Cost Details APIs, it exposes to more detailed, near real-time information about how the consuming resources is and, ultimately, spending money. Current meter rates and tailored pricing is given by Pricing APIs, which can be used for a more precise forecast and budget. Using the Budgets and Alerts APIs, users can set limits on spending and set up automatic alerts, providing greater financial control across projects. The Invoicing APIs also allow access to rich billing information such as invoice summaries and transaction level information which enables a transparent and accountable billing system for transactions. Finally, the Reservation APIs enables customers to manage their reserved instances by providing transaction history and personalized recommendations on future reservations to get the best savings. Collectively, these technologies make it possible for businesses to automate their financial processes and optimize them with Azure.

VI. Flexible Pricing Model

The following are some pricing models with different operational and financial purposes:

- Pay-As-You-Go
- Reserved Instances
- Spot Instances

Microsoft Azure offers the broadest range of pricing options that match the needs of the applications and the realities of the workloads that are running. The most flexible Pay-As-You-Go model, where customers can pay for what they actually consumed for each consumer, it's very suitable for those applications and services with non-predicted and cyclically unexpected loads. For more predictable workloads, Reserved Instances unlock more savings as purchasers commit to one or three years for services, such as virtual machines, thus driving greater long-term efficiencies. This model is highly advantageous for workloads with known resource needs. Also, by using Spot Instances, organizations can leverage unused Azure capacity at highly discounted prices while continuing to benefit from the reliability that comes from running workloads on Azure. These pricing options provide businesses the flexibility to align their cloud spend with usage patterns and project needs.

VII. Billing and Invoicing Management

Azure Billing processes and governs billing on the cloud efficiently by giving the ability to manage subscriptions, set spending limits, and enables to create detailed reports so that can give customers the detailed report they need. These features provide that finance teams and company management are transparent and accountable for their actions, contributing to informed decision-making.

VIII. Cost Optimization Tools and Techniques

Microsoft Azure provides several out-of-the-box capabilities to assist organizations in minimizing unnecessary costs:

- Free Services
- Azure Advisor
- Savings Plans and Reservations
- Azure Hybrid Benefit

Microsoft Azure comes with its set of tools and mechanisms dedicated to assist businesses in reducing needless loss of funding as well as optimizing cloud savings. About the free services, Azure comes with some free services, some can be used indefinitely others can only be used for a certain period of time and under certain conditions; organizations can leverage this to optimize its' cost. Azure Advisor is a personal recommendation tool that provides information, such as: Best practices and recommendations with regard to security, performance, of high availability based on organizations usage patterns to help maximize the value of its' Azure subscription. For long-term planning, Savings Plans and Reservations provide significant cost savings — up to 72%, compared to On-Demand pricing , in exchange for a one or three-year commitment with specific usage requirements. Furthermore, Azure Hybrid Benefit makes it possible to re-use on-premises licenses for Windows Server, SQL Server, and supported Linux distributions in Azure, which should remove a significant portion of those pesky transition costs to the cloud anyway. Together, they provide organizations with the tools to run effectively and ensure they have an eye on their pockets when executing cloud strategies.

IX. Strategic Cost Optimization Practices

To maximize cost efficiency, organizations should adopt these best practices:

- Resource Rightsizing
- Auto-Shutdown Policies
- Tool Utilization

Azure cost-efficiency best practices and here are a few best practices to be followed to ensure the best cost optimization in Azure. Also, resource rightsizing is critical, wherein companies should be able to periodically review and then adjust how much computed resources have been allocated to the amount of actual use, so that they don't waste money on over-provisioning. An additional effective method can be to assign auto-shutdown policies for

non-compact workloads, and thus sufficient no costs for idle resource consumption, particularly out of hours. Organizations can also maximize the use of Azure's native cost management tools, defining clear budgets, tracking spend and heeding optimization suggestions from services such as Azure Advisor. Enterprises can control their cloud spending more effectively with these strategies, to ensure they maximize their operational efficiency over time.

By using Microsoft's comprehensive Cost Management tool along with best practices for managing operations, organizations can achieve full visibility into organization's cloud spend, enforce cost governance, and ongoing optimization of organization's Azure for financial and operational efficiency.

3.1.2 Security

Security is one of the major concern in information systems and network management and has an important role in reducing the problems of unauthorized access, exploitation, interruptions and information loss. As cloud computing revolutionizes traditional IT operations, security measures in cloud are somewhat different from those in on-premises platforms. The dynamic and geo-distributed nature of cloud services, where microservices span the globe and are interconnected over networks, calls for a more sophisticated multilayered security architecture. Data security in this case requires preserving various aspects of the environment, such as; network, application layer, architecture, and user identity.

Security in cloud systems like Azure can be considered at three fundamental levels. The first one is about cloud security – here users would like to keep whole cloud secure, all that ecosystem, plus users would like to make sure that each exposed micro- service from the cloud is secure too. This encompasses user identity verification and encryption methods. The second level is in app/microservice security, taking an emphasis on securing APIs, the app code, and the data flow between services. The last level is the infrastructure layer of microservices architecture, where products, such as Cloud Security Posture Management (CSPM) and Cloud Workload Protection,

come into play. CSPM tools play a key role in detecting misconfigurations and enforcing compliance particularly in multi-cloud and hybrid settings. Cloud Workload Protection is concerned with protecting applications, its data, and the underlying infrastructure on various platforms. It need to consider workload security as shared responsibility model in the cloud systems.

Security Framework of Microsoft Azure

Azure takes a layered and holistic approach to security, which extends across infrastructure, data, applications, and identity. This approach incorporates integrated tooling, intelligent threat detection, and global compliance for a secure business platform.

I. Network Security

The Azure network security model is focused on controlling and protecting traffic to and from assets. Key components include:

- Azure Firewall
- Network Security Groups (NSGs)
- Distributed Denial of Service (DDoS) Protection

The Azure network security model is built to protect cloud-environment resources by controlling and filtering traffic flowing into and out of the environment. At the heart of this model is the Azure Firewall, which is a cloud-native, stateful firewall service that provides traffic management, protection, and intelligent threat identification for both outbound and inbound traffic across multiple workloads. It's built to be scalable and fault tolerant which provides protection over time as demand ebbs and flows. Another important concept is NGS (Network Security Groups) – which users can use, define detailed access control policies based on IP, protocol, and ports. These groups are used to enforce security boundaries by allowing or denying traffic between resources in Azure virtual networks and isolating important workloads. Moreover, Azure has on the backbone DDoS (distributed denial of

service) Protection to mitigate and protect from volumetric attacks. This is a service that keeps applications available and responsive even during large surges in popular or when they are attacked, so users can maintain performance and operational continuity.

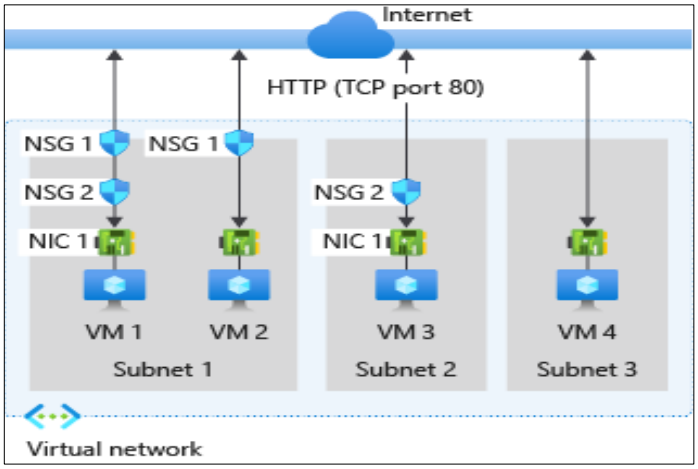

Figure 2: Azure processes inbound and outbound rules for network security groups

Source : Microsoft (2025)

II. Data Security

Data security in Azure ensures protection at rest and in transit. Azure leverages several key technologies:

- Encryption
- Azure Key Vault

Azure provides strong data protection features to secure data, at rest and in transit. For safeguarding data at rest, Azure leverages Storage Service Encryption (SSE), which not only encrypts data as it is written to storage but can also decrypt it automatically when the data is retrieved, so users don't have to manually ensure that sensitive data is protected. The data transferred between systems is transferred via secure transport (TLS) to ensure that in-transit information is secure and can't be captured or tampered with. Also, Azure offers higher security for data with the Azure Key Vault, a service to secure keys, secrets and

certificates. This facility lets applications and services securely acquire and utilize an encryption key, so that organization's sensitive data can be kept secure from unauthorized use. These technologies combined represent a complete data protection framework across all phases of data at rest, in transit, and on device in Azure.

III. Identity and Access Management(IAM)

IAM in Azure is foundational for controlling and auditing access to resources. It supports several capabilities:

- Azure Active Directory (Azure AD)
- Role-Based Access Control (RBAC)

Identity and Access Management (IAM) is one of the critical security controls used to protect cloud resources which is to allow only the correct user to have the right access in Microsoft Azure. The foundation of Azure's IAM system is Azure Active Directory (Azure AD), an all-embracing identity management service that provides Single Sign-On (SSO) functionality, allowing users to sign in to multiple applications using a single identity. It also provides support for Multi-Factor Authentication, to add an additional authentication layer, and conditional access policies, that allow users to dynamically enforce access requirements based on user context, like location or device state. Role-Based Access Control (RBAC) is then added to the picture to provide for more granular-level permissions an organization might want to enforce. With RBAC, it gives users the least permissions needed for them to do their job, and reduces the risk of someone doing something they shouldn't. When combined, these IAM capabilities allow enterprises to retain control, visibility, and accountability over who has access to what across their Azure deployment.

IV. Application Security

To protect hosted applications, Azure incorporates advanced security tools:

- Azure Security Center
- Web Application Firewall (WAF)

Microsoft Azure protects the applications that are running on it by incorporating a powerful set of application security detections and mitigations which help secure applications against threats and against vulnerabilities in the application itself. The Azure Security Center is an indispensable part of this story providing centralized security management for Azure along with hybrid clouds. It will watch resources all the time, find potential security risks, and even suggest how to make users resources more secured. A different Azure service provides security for web applications, the Azure Web Application Firewall (WAF), which guards against the most common web vulnerabilities, including SQL injection and cross-site scripting (XSS). These exploits are commonly directed at an application layer to compromise data or functionality. WAF helps to enhance the security and stability of web applications by monitoring and examining HTTP traffic, serving as a shield against malicious inputs. Combined, these solutions offer a robust defense layer that protects applications against emerging cyber threats.

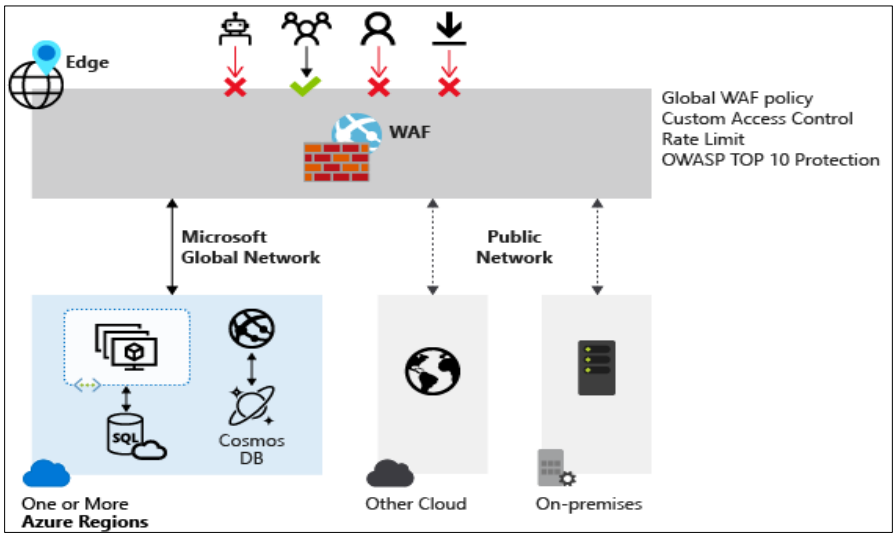

Figure 3 : Web Application Firewall(WAF)

Source: Microsoft, 2025

V. Compliance and Governance

Azure promotes regulatory adherence through integrated governance tools and broad compliance certifications:

- Azure Policy
- Compliance Certifications

On Microsoft Azure, compliance & governance is enhanced through native-in tools, complete with vast certification coverage, that help enterprises to meet their regulatory and operational standards. Now, one of the most important, this particular tool is Azure Policy which is a service that permits companies to generate, distribute, and enforce policies controlling the use and configuration of resources. This is to help enforce the application of organizational standards, maintaining compliance at scale. In furtherance of investment in secure and transparent operations, Azure has many compliance offerings, such as globally recognized standards as ISO/IEC 27001, SOC 1/2/3 and General Data Protection Regulation (GDPR). These certifications confirm that Azure follows stringent protocols for data protection and security. In addition, Azure provides custom compliance assistance for the most challenging environments such as SAP systems, or other mission-critical workloads, with risk-assessments and recommendations for secure deployment, as well as ongoing compliance scanning. This end-to-end process enables customers to confidently work in regulated industries with strong security and governance.

VI. Threat Detection and Incident Response

Azure strengthens proactive threat detection and response with specialized tools:

- Microsoft Defender for Cloud
- Azure Sentinel

- Incident Response Planning

Microsoft Azure further improves a robust security posture through advancements in monitoring and alerting tools for active threat detection and response, detecting and responding to security risks in a timely manner. Central to this approach is Microsoft Defender for Cloud, a single, integrated security solution that extends end-to-end security across Azure, on-premises, and multi-cloud environments. It continually scans resources for security compliance based on the security benchmarks that are defined and provides prescriptive recommendations for mitigating those security vulnerabilities. And, to build on this Azure Sentinel is a scalable, cloud-native, Security Information Event Management (SIEM), offering intelligent security analytics with out-of-the box data connectors and unmatched threat intelligence. It facilitates the continuous monitoring, detection and hunting of threats anywhere across the enterprise. Azure also heavily promotes incident response planning, and walks organizations through creating formal policies for identifying, analysing, and reacting to security incidents. These response options facilitate immediate containment and remediation to reduce the impact of threats and keep the business running smoothly. Together, these deliver unified visibility and synchronised defences that are crucial to securing today's complex cloud environments.

VII. Physical and Infrastructure Security

The physical infrastructure of Azure is secured with a multi-layered security model. Microsoft global data centers are designed to limit unauthorized access, and for physical resiliency:

- Controlled Access
- Facility Perimeter and Surveillance
- Redundancy and Resilience

Datacenter Security – Physical Security and Resiliency, Microsoft Azure provides the physical security and financial structure of its infrastructure that includes a range of protections that provide secure datacenter facilities that block unauthorized access, environmental and electronic elements to the data center. Access Control – Organizations uphold controlled access protocols, and all require prior authorization, a legitimate business case, and escort only policies to the data center. This keeps the distance away from any physical penetration at an unauthorized distance. The perimeter of the premise is protected by strengthened fencing, and is under 24 hour surveillance of trained security staff they work with day and night advanced CCTV systems. To ensure service availability, Azure is built in redundant and resilient components, such as backup power supplies, redundant cooling and fault-tolerant network settings, so that service can be continuously delivered even when fault takes place. These systems were designed to ensure that Azure services are available despite hardware or environmental failures. Microsoft uses a defense-in-depth approach to protect the physical, operational, and systems-level layers of the cloud infrastructure. This depth of security model represents Microsoft's strong commitment to the protection of customer data and the security of global infrastructure.

Conclusion, by integrating comprehensive and layered security into it's cloud solutions, Microsoft Azure tackles today's security challenges across multiple deployment models. Azure incorporates industry leading solutions related to network security and identity management to access compliance and physical security to deliver industry-leading practices and technologies to safeguard enterprise workloads. This end to end security model helps ensure the privacy and integrity of company data as well as being able to take advantage of the scale, agility and reliability of the cloud.

3.1.3 Performance

Performance is indeed a key factor in the successful operation of cloud applications and services. In Microsoft Azure, performance efficiency is the capacity for the needed system resources to be provided at the right time (to service the load) even as the load changes, so the system can be

responsive to varying levels of demand (load) quickly and resource consumption can be streamlined. A few ingredients in the soup of performance management are revolving capacity (scale out and scale in for resources), discovering and addressing performance hotspots, and optimizing the application and infrastructure sources to have the system hum.

Optimizing the network performance is the foundation for achieving low latency and responsive services hosted on Azure. Unfortunately, a performant operator must take the network and storage resources into account, as they affect the response time of the application. The choice of the appropriate networking resources virtual networks, bandwidth tiers and routing patterns enables good communication between services. Adding a middle layer of messages allows to scale out more layers between services and makes capable to do that without losing performance in the architecture of Azure. This inner layer serves as a staging area, facilitating queuing and asynchronous processing of incoming requests from services. Even when a service lags behind, the buffer ensures no requests are lost and operations and user satisfaction is smoother.

Storage utilization is also an important factor in the improvement of the overall performance of the application. In large scale cloud deployment, data is often partitioned so as to facilitate better manageability and accessibility. A good partitioning policy can reduce contention, resource competition, enhance scalability and throughput. Also, caching aids in minimising the latency associated with data read. Caching can be provided on various levels of the architecture, between the database and the application servers and between users and the web servers. For instance, caching static content (e.g., images or webpages) closer to browsing users not only fastens the delivery of the content, but also reduces load on backend systems which in turn enhances the performance for other users

Azure's Holistic Performace Management Strategy

Performance Tuning for optimising performance in Azure, Microsoft uses a combination of hardware-based optimisations like proprietary hardware-related tweaks, as well as software-based tuning mechanisms. This makes certain that apps and services running on Azure services are efficient, highly responsive and can scale equally well across all modes of operation.

I. Infrastructure Optimization

In addition to software-level improvements, Azure has invested in custom-built silicon and infrastructure to level up performance at the hardware level. Advancements such as Azure Integrated Hardware Security Module (HSM) and Data Processing Units (DPUs) seek to enhance compute efficiencies and lower the latency, especially for specialized workloads like AI and big data analytics. These special components help to better optimize, and secure processing workloads in the Azure datacenter.

II. Continuous Performance Monitoring and Tuning

It is important to pay attention to the behaviour of the system in terms of performance management. Azure provides users with different options for monitoring to collect and look at performance data like CPU Usage, Memory Usage, Disk I/O and Network Throughput. Organizations can use these learnings to identify early bottlenecks and make changes in time e.g., optimized code, added resources, etc. Regular performance checks ensure ongoing service levels and they are the opposing response to system degradation.

III. Scalability and Load Management

The cloud resources are automatically scaled out or in with widespread auto-scaling capabilities supported by Azure. This scaling up and down ensures that applications are available as needed and then reduces back down when not in use. Auto-scaling improves system responsiveness and helps in cost reduction by avoiding overprovisioning.

IV. Data Storage and Access Efficiency

Although it depends on the needs, Planning the right storage solutions are important to get the best performance of data. Azure has a variety of storage options beyond blob storage, including managed disks and premium SSDs, which users can optimize for their workloads. The configuration of these storage services have an impact on latency and data retrieval times. On top of that, the method of managing the data structures and access rules optimizes the speed and resource consumption of queries.

V. Educational Resources for Performance Best Practices

In an effort to further assist developers and IT professionals on performance optimization, Azure has supporting guided learning plans around reliability, security and performance tuning. These guided modules provide tools and resources for users to work with their organizations to accelerate the use of Azure. They're a great resource for teams that are looking to adopt best practices and create a robust cloud solution.

In summary, by optimising performance across several dimensions - such as infrastructure improvements, monitoring, scale out, and storage efficiency - Microsoft Azure provides a comprehensive framework in preserving high application responsiveness. With the custom hardware and intelligent tools of Azure, businesses are equipped to adapt to evolving demands, pushing the envelope of what cloud can do so they can do more for their customers.

3.1.4 Scalabity

Scalability is a fundamental design principle in cloud computing to accommodate the dynamic fluctuation of workloads while maintaining the desired performance and efficiency. Microsoft Azure comes with strong support for elasticity features whether it is manual or automated resource management to scale the infrastructure on real time work load. Microsoft Azure facilitates to meet the demand surge of customers, developers and IT professionals have been looking for tools and guidance to keep services healthy, manage costs and throughput, and delight their users with responsive applications – even when under heavy load or when sitting idle.

I. Scaling Approches in Azure

- Vertical Scaling (Scaling Up/Down): It modifies the resources organization already have by increase/decrease in capacity (CPU, RAM, DISK, etc…) For example: it is now easy for applications to upgrade to a higher performing VM size / pricing tier to meet increased performance needs. This is simple approach, but the maximum load of the new resource could be restrictive.

- Horizontal Scaling (Scaling Out/In) spreads demand across instances of resources. Azure comes with utilities like Virtual Machine Scale Sets, which provide the automatic scaling of VMs based on real-time consumption. This provides the benefit of fault tolerance and enables applications to better manage sudden traffic increases by distributing the load across different instances.

II. Azure Auto-scale

In order to automate the process, Azure offers Auto scale, which automatically scales cloud resources up or down, depending on performance needs, provisioning additional resources when they're needed and de-provisioning them when they are not. Also known as auto-scaling, this would remove the human element from deciding when to scale the infrastructure, and scaling would be done automatically when the load changes. Auto-scale provisions additional resources when demand for applications increases to maintain performance and SLAs. When the demand drops, the unused resources are automatically freed to save the cost.

It is enabled by the cloud's elastic infrastructure, for preserving performance and diminishing resource management overhead. It has the effectively of providing/releasing capacity to occur without knowing by the user and without having a human involved in it (within the use of the workload).

III. Implementing Auto-scale

- Configuration: Under consideration aspect, the autoscaling rules can be defined on CPU, memory, or custom rules such as a time schedule. For instance, it can configure an app to scale out when CPU usage is over 70% and scale in when CPU usage is lower than 30%. Because of these rules, that resource is added or subtracted at exactly the right time to give the best performance and operational cost.

- Resource support: Azure Auto-scale supports a variety of resources. For example, it can use it to scale App Services, Virtual Machines and Cloud Services, and users can scale

across different application architectures. This degree of flexibility enabled bringing auto-scaling not only to users webapps, but also their background processing work.

IV. Best Practices for Scaling in Azure

- Monitoring & Metrics: It would be better to know how the app performance in order to scale it in the times it is demanded. Azure Monitor delivers comprehensive system-wide performance monitoring and resource utilization details that help teams to establish meaningful thresholds and scaling rules.

- Testing scaling policy: Before configuring scaling to production, it is recommended to test and understand scaling by simulating load. This testing has the added bonus of ensuring that users' scaling policies behave properly in different conditions and don't go off and do weird stuff by accident.

- Cost Management: Apart from shrive scale costs, auto-scale is intended to right-size resource provisioning, and infinite scale out is also not a cheap party. The key takeaway here is that resource limits should be put in place and the scaling strategies must be reviewed to prevent an imbalance of performance and cost.

As a summary, Azure's scalable model is a great way to create applications that are resilient and fast responding and that can up and down scale as people need. Using vertical and horizontal scaling, in combination with automation tools such as Azure Auto-scale, a business can ensure predictable service performance and efficient operation. Implementing best practices in scaling, whether in terms of performance monitoring, thresholding, or cost control ensures that the apps will keep up with today's performance needs and scale as it scale up. For these reasons, with Azure's end-to-end scale out choices are key to delivering cloud-native agility and long-term infrastructure sustainability.

3.1.5 Downtime/High Availabilty

Service continuity and minimisation of downtime are key aims of contemporary digital infrastructure, irrespective of their age. Microsoft Azure works to address these concerns by offering a combination of high availability (HA) features and architectural design patterns that enable applications to run non-stop in the wake of hardware failures, maintenance, and even datacenter outages. Azure's strategy is to employ physical redundancy, intelligent distribution of workloads, and automated scaling in combination with durable data protection, to deliver a resilient cloud that supports mission critical service levels.

I. Azure Availability Zones

A key to high availability in Azure is its Availability Zones, separate datacentres within the same Azure region. Each zone has its own power, cooling, and networking which gives true fault isolation. Organizations can protect their applications and workloads from datacentre-specific outages by distributing services across multiple Availability Zones. This multi-Zone approach means that if one zone is down, the other will still remain operational thus ensuring application uptime and availability.

II. Availiablity Sets

For the intra-datacentre fault-tolerance needs, Azure gives the option of Availability Sets. This feature allows the VMs in application to be deployed in such a way that they will automatically be distributed across different fault domains (different physical servers and racks) and upgrade domains (used when Azure schedules a maintenance operation). This is enough spreading so that hardware failure or platform update doesn't affect all VMs at once but minimizes the risk of downtime. So, Availability Sets are a good fit for apps that require both predictable performance and a level of protection against local hardware failures.

III. Virtual Machine Scale Sets

For workload types that require dynamic scaling and high availability, Azure provides Virtual Machine Scale Sets (VMSS). By enabling easy creation and management of a group of identical VMs as a unit, the feature is able to automatically increase or reduce the number of VMs in use, in order to handle workload needs, or for example as part of a scheduled job. Scale sets are not only fault domain, update domain or Availability Zone aware to provide resiliency, but also resilient and traffic intelligent when it comes to apply different ratio to different traffic. The VMSS ideal for large-scale applications that benefit from ease of VM management, better resource utilization, and reduced overhead of inter-VM communication.

IV. Load Balancing

Availability is improved with Azure powerful load balancing that balances the incoming network traffic to multiple instances of services or applications. That way no single server gets swamped and it's always responsive. Azure offers multiple load balancing options, including Azure Load Balancer for the transport layer, for ultra-low latency and high throughput, and Application Gateway, a layer-7 load balancer that provides powerful and fresh application delivery capabilities. These can be used to prevent Single Points of Failure (SPOF) as well as achieve transparent failover of backend resources.

V. Data Redundancy

High availability also requires data durability, something Azure achieves by providing multiple ways to guard against data loss and preserve continuity:

- Locally Redundant Storage (LRS) is replicated three times in a datacentre.
- Zone-Redundant Storage (ZRS) replicates users' data across three Availability Zones in the same region, so it is resilient to an AZ failure, thus users' data remains available in that case.
- Geo-Redundant Storage (GRS) The most redundancy available by replicating data to a secondary geographical region - GRS protects against region-wide unavailability.

With storage redundancy options, businesses can select the degree of data protection they need to ensure their business continuity planning protocols.

VI. Service-Level Agreements(SLAs)

Azure backs its high availability solutions through comprehensive Service-Level Agreements (SLAs) for assured availability and service uptime for different services. The best uptime percentages can be achieved using Azure's SLAs, if solutions are designed with more than one HA feature (i.e., availability zones, redundant storage, and autoscaling, etc.) These guarantees ensure that important services will continue to be available and perform well during unexpected events.

In summary, the Microsoft Azure high availability infrastructure is layered with fault-tolerant, automatically managed resources, load balancing, and strong data protection in place. Using Availability Zones, Availability Sets, VM Scale Sets and numerous strategies for redundancy, Azure architectural designs for cloud-based applications are reliable through failure and designed for robustness. These features, in conjunction with robust SLAs and performance-monitoring tools, allow organizations to build reliable, scalable, and fault-tolerant systems in the cloud and reduce the downtime their indicators see and their users experience.

3.1.6 Governance

In the fluid digital world, it is very important to have a good cloud governance in place to have control on the cloud environment, maintaining compliance, and operational efficiency. As stated in Microsoft Azure (2024), the govern in Cloud Adoption Framework (CAF) approach provides comprehensive, structured model for governance and in institutions at cross different industries. The framework covers important categories including security, compliance, operations, cost management, data protection, capacity planning, and the human aspects behind the responsible use of AI.

Cloud governance is a discipline dedicated to establishing and maintaining cloud computing policies and the processes with which to monitor their continual effect. It creates a collection of guardrails

(policies, procedures, and tools) that govern and standardize how cloud environments are accessed, configured, and used. These guardrails ensure that cloud use is in line with corporate policies, so employees cannot engage in unauthorized or unmonitored use cases that can result in security holes, compliance violations, or operational inefficiency. Defining what is acceptable behaviour and putting in systematic controls will allow organizations to have a secure and adherent cloud.

I. Importance of Cloud Governance

Effective cloud adoption is underpinned by strong governance that ensures productivity and security. Without it, organizations may wind up dealing with unexpected challenges, like security incidents, policy violations, cost overruns, or sloppy resource utilization. Proper cloud governance mitigates these risks by setting standards on how services are deployed, monitored, and maintained. It also codifies that cloud usage is consistent with the larger business, so teams can innovate and scale rapidly without sacrificing control or compliance.

II. The Continuous Nature of Governance

Cloud governance isn’t a set-it-and-forget-it exercise, it's an ongoing activity that needs to change as new technologies emerge, new regulatory demands become clear, and organizations change focus. In order to facilitate good governance, organizations need to review their governance practices, monitor compliance, and make changes, if required, on an ongoing basis. Microsoft’s CAF Govern approach is structured to facilitate this back-and-forth by providing a five-step framework to develop, apply and maintain solid governance over time.

III. Five Key Steps in Azure Cloud Governance

Build a Governance Team: The very first step is to create a governance team that will set policies, oversee implementation and report back on governance progress. This cross-functional team includes members from IT, security, compliance and operations and looks at things from the broadest view possible.

Assess Cloud Risks: Review a company's catalogue of cloud interconnections to assess any risks they may bring. These should evaluate risks across domains ranging from security, regulation, operational, financial, data governance and AI deployment. Azure offers a range of tools and services to aid in evaluating and prioritizing these risks in a way that is appropriate for the organization.

Document Governance Policies: What good is flagging a risk, if users don't have a governance policy to handle the risk? These policies serve as a piece of formal instruction for any party involved, but they also set rules of behaviour, and establish what is expected from a point of view of secure, compliant and efficient cloud usage.

Enforce Governance Policies: In order for policies to be effective, actions must be taken to enforce them. Azure provides tools, such as Azure Policy and Azure Blueprints, that can help automate rule enforcement and achieve uniform compliance across the cloud estate. Manual review can also take place in cases where automation is not feasible.

Monitor Governance Compliance: Continuous monitoring is essential to detect non-compliance, audit the use model, and refine governance. Azure's built-in monitoring can be set up to alert when there is a policy violation, providing a fast remediation and helping to keep any true governance posture.

In summary, the Microsoft Azure governance model as described in the Cloud Adoption Framework (CAF) offers a scalable and adaptable way to maintain control and achieve efficiency in use of the cloud. Solid governance aligned with business operations by defining roles, performing detailed risk assessment and documentation of policies, and the automated enforcement and control to support, and oversee it. By making governance a continuous practice, businesses can ensure that their cloud is secure, compliant, and that it is working with, instead of against, their broader long-term strategy.

3.2 On – Premise Computing Architecture

3.2.1 Cost

Implementing and operating an on-premises IT infrastructure requires a considerable level of financial and operational investment. Unlike cloud options, on-premise systems means that companies have to maintain their own physical servers and data centers, which involves major upfront and ongoing costs. Sosnovyk (2024) suggests that companies who use on-premises setups should consider ongoing costs like electricity, space, and hardware maintenance which all lead to high operation costs.

One of the most significant aspects of an on premise infrastructure is the large expense that comes with purchasing an in initial setup. As highlighted by Orgizit. com (2025), including acquiring of hardware and software, and installation of a physical machine power and cooling. In this way, the price of courses for the cloud infrastructure mode is repaid with the first build, because a build must use the full computing and the storage capacity of the cloud (Vassilenko, 2019). That's opposed to cloud solutions, which offer customers subscription-based package, with customers paying over time.

Yet there is a price to pay for on-premises infrastructure that is well-suited to some businesses, particularly large organizations. Capital and time to invest are significant up front, but for organizations with usage needs large enough, owning and operating their own resource will often dominant in the cost-benefit equation. Vassilenko (2019) observes that, in-house maintenance costs may remain lower than the sum of annual fees for cloud services.

In real world terms, running infrastructure on premises requires a talented and focused systems team. Selection of experienced staff to manage Setup, configuration monitoring and upgrades to the system by the organization. Personnel training is the key to successful operation and to handle specifics like hardware choice, software installation and networking. There is also the cost for software licenses for several enterprise applications, and the cost of power consumption and staff

salary. Moreover, businesses have to purchase power backup systems and cooling equipment to keep systems online and infrastructure safe.

Another issue is the requirement of more and more frequent hardware upgrades (or even change) as the technology progresses and the performance requirements are raised. Enterprises have to invest in cost-intensive hardware components to serve certain workloads. The building and maintaining of infrastructure is capital-intensive, but it also requires strategic planning and technical supervision (www. fs. com, 2025).

As a conclusion, while there are substantial upfront and ongoing costs associated with on-premises infrastructure, high scale organizations that value control, customization, and cost savings in the long term will realize tangible benefits over an extended period of time. Adopting either an on-premises or hosted model must be a decision based on an organization's evaluation of workload requirements, budgetary limitations and the ability to manage in-house IT infrastructure.

3.2.2 Security

For many organizations, especially those managing regulated data or highly sensitive data, the on-premises infrastructure is preferred because of the greater security and control that it provides. As Sosnovyk (2024) states, companies prefer to keep personal records (eg, banking, personal identifiers) in their own facilities since they prefer not to involve third parties when it is possible. This is especially important in industries such as finance and government where there are strict data protection requirements in place and outside hosting may not be an acceptable risk.

In a traditional security model, everything is kept inside in house within a private environment and no data is transferred or processed outside that environment on a public network. This isolation dramatically reduces the exposure to external cyber threats. In this context, the main goal is to avoid unauthorized access to a company infrastructure. In order to do this, organizations often implement firewalls, VPNs, user authentication systems, and other security products to create controlled access and to protect key assets. Due to the fact that data in these environments is not sent over the internet via proprietary frequency broadcasts and modulations there is less of a set

requirement for advanced encryption but a basic and still effective form of network security. Hence the general information security risk in traditional on-premises environments is typically less than in the cloud.

The major advantage of this architecture is the complete control that is given to the users. Administrators can monitor the system in real time, keep track of users' activities and take immediate action at the sight of anything suspicious, such as stopping an action or quarantining a piece of the process. This feature facilitates very responsive and adaptive security stance. Also, organizations can create and implement their security policies based on their regulatory and internal standards and not depend on third-party configurations, commonly found in cloud platforms (Sosnovyk, 2024).

However, on-premises infrastructure comes with its own risks. Physical Security – Natural disasters: Natural disasters could easily destroy or compromise a business asset, a malicious act of nature could result in the destruction of hardware assets. Furthermore, insider threats, in which employee disclose or transfer sensitive information to competitors, are also a significant weakness. There are also continuing on-premises operating expenses, such as system patches, staff training, and hardware maintenance (Nikita, 2024).

Whether it is for public authorities or financial institutions, the heightened level of secrecy demands "keeping things within closed doors," or on-premises, which is paramount for abiding by the rules and regulations of privacy and standard of ethics by law. These industries rely on highly personalized and secured IT environments to maintain public trust and operational integrity., Ramachandra et al. (2017) and Pahl et al. (2013) say that data security and privacy as they pertains to all industries represent one of the top-rated agendas therefore, although maintaining a security system on-premises is costly, such a system is more assuring to clients and stakeholders.

For strong protection, companies with on-premises system are advised to roll out wide security controls. These can involve firewalls, intrusion detection systems (IDS), encryption, access controls, network segmentation and periodic security assessments of the on-premises data gateways (www. fs. com, 2025). These practices contribute to a secure, compliant and controlled IT environment,

instilling confidence with clients who have relied on on-premises data management solutions for long periods of time.

Conclusion On-premises infrastructure demands large capital investments and day-to-day operational scrutiny, however it delivers unparalleled control and customized security to organizations that can't risk confidentiality exposure. The capability of managing all data attending internally makes it a good candidate for corporations where data security is critical.

3.2.3 Performance

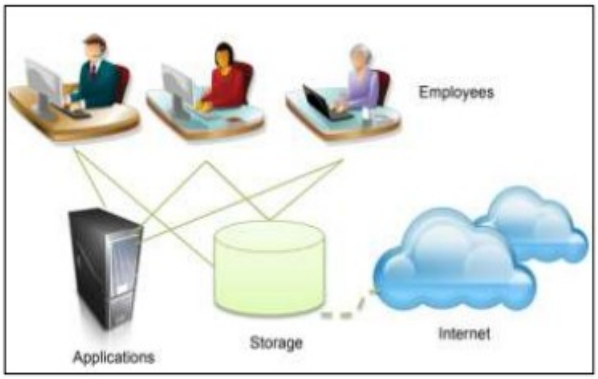

Figure 4 : On Premise Working Environment

Source: Shaina, Arora and Kaur (2023)

On-Premise computing can offer better performance for specific applications, such as those that require a lot of processing power or need to be accessed offline (TECHVIFY,2025).Everything it hosts is highly responsive for on-site users. Teams can fine-tune hardware performance to meet specific needs. Specialized networking equipment and software settings can be used. Customization is often required. Significant equipment investment and a skilled technical team are essential to optimize your system for maximum performance. Ongoing optimization is essential. Regular updates and fixes are necessary. Requires regular updates, troubleshooting. Constantly check infrastructure and system logs. Define and manage business continuity plans. Tailor the setup to meet specific needs.

On-premises data centers allow teams to retain complete control over their data. Watch for breaches, leaks, and data corruption(www.fs.com, 2025).

As a professional communications equipment and solutions provider, on premise data center customization is committed to providing high-performance data center switches and a professional modern solution team. On premise data center switches and servers provide flexible customization, which can customize hardware configurations (such as memory, storage, processors, etc.) and network configurations (such as multiple network cards, network security Settings, etc.) according to specific requirements. Help you maximize resources and improve business efficiency to precisely meet your specific needs(www.fs.com, 2025).

3.2.4 Scalability

Scalability is an important consideration in IT infrastructure investment plans and has a profound impact on how well a company can react to changing workloads and market requirements. Moreover in the on premise world, true scalability is neither easy nor cheap to accomplish. As noted in TECHVIFY (2025), scaling out on-premises infrastructure entails the purchase and implementation of more hardware and software so that it is time-consuming and expensive.

The scaling process of an on-premise systems whether vertically (making existing components more powerful) or horizontally (adding more server) requires several steps that can disrupt business. Expanding capacity often requires shutting down systems, inserting new parts, and reconfiguring server values. This results in inevitable downtime, along with a long turnaround time for purchase and installation, which ultimately affects the business agility. Furthermore, when the necessity arises to scale back down, companies are forced to shut down servers and physically remove hardware they previously invested in but are no longer using, thus ending up in a situation with unused investments.

On-premise data centers are also limited by physical factors, including available floor space, amount of power and cooling. Such limitations can be an impediment to further growth, particularly when growth needs to occur quickly or at a large scale. According to www. fs. com

(2025), these restrictions render on-premises infrastructures unsuitable for scenarios with spikey traffic or unpredictable usage patterns when supply cannot be forecast or controlled.

Even more it is difficult tying structures to permanently moving resource requirements. As www. nordlayer. com (2024) further indicates, business requirements change frequently and sometimes it is hard to match them with fixed hardware capacity. Surges in demand can cause systems to become overloaded, and unanticipated decreases in usage can make expensive infrastructure sit idle. This inflexibility reduces the ability of the business to adjust its operations to take advantage of growth opportunities or cope with unexpected changes in operations.

On-premises infrastructures are more static, therefore slower, when compared to cloud environments where all resource levels can be borrowed or returned in real time. The scaling up or down process is limited by logistical, financial and physical constraints, making it difficult for companies to be agile in competitive and rapidly changing markets. For the companies having varying customer needs, transferring to on-premise may not be cost-effective or efficient enough to be competitive (www. fs. com, 2025).

Finally, on-premises infrastructure, while it may provide control and security benefits, isn't able to scale. Aligning hardware to dynamic business requirements is difficult, the costs and operational implications of scaling were traditionally prohibitive. Therefore on-premises computing is a less agile choice for contemporary organizations. These restrictions have to be offset by an organization considering infrastructure strategies, especially in an environment requiring high flexibility and quick response.

3.2.5 Downtime/ High Availabilty

Organizations must implement strategies to minimize service interruptions and ensure continuous system operation. On-premise solutions require dedicated hardware, software, and operational strategies to handle failures effectively.

Downtime Considerations in On-Premise Systems Causes of Downtime:

Hardware Failures: Physical components such as servers, storage devices etc. can fail due to aging, overheating, or power issues (Weaver, 2013). Software Issues: Operating system crashes, misconfigurations, or security vulnerabilities can cause outages (Smith et al., 2020). Power Outages: Disruptions due to electrical failures or natural disasters (Marwah et al., 2010). Network Failures: Internal network congestion, misconfigurations, or failures in external connectivity (Al-Shabibi & Wang, 2013). Human Errors: Misconfigurations, improper updates, or accidental shutdowns contribute to unexpected downtime (Weaver, 2013). Following strategies can be used as implementations for High Availability in On Premise systems:

- Load Balancing can be done through distributed network to balance traffic across multiple sever. But this is a expensive implementation for an organization.
- Automated Backup and Disaster Recovery through regular back up plans.
- Implemnet Virtualization and Live Migration via Virtual Machines and etc to prevent downtime during maintaince or failure.
- Using RAID(Redundant Array of Independent Disks) prevent data loss due to hard drive failures.

3.2.6 Governance

Governance is a significant factor in the management of IT infrastructure, in particular ensuring compliance with industry regulations. Organizations using on-premises solutions are fully responsible for complying with all applicable laws and regulations. According to TECHVIFY (2025), organizations need to be proactive about compliance across the business operations, as the consequence of non-compliance could be legal retributions and reputational risk to the organization.

Just about all businesses face some form of government control, whatever industry they are in. Examples including the Health Insurance Portability and Accountability Act (HIPAA) which regulates confidential health information and the Family Educational Rights and Privacy Act (FERPA) which

governs confidentiality of student records. Organizations working within these frameworks are mandated to follow the predetermined requirements of those regulations in the manner that they handle and process data (Sosnovyk, 2024).

Local computing and storage are particularly advantageous in this concept, as data can be stored and processed locally, giving organizations a high degree of control. As Nikita (2024) noted, in-house data storage streamlines compliance obligations by not relying as much on third-party service providers and enabling firms to implement and enforce their own security and privacy requirements. This local security model reduces compliance risks and powers direct compliance with local regulations.

Compliance also means establishing the toughest governance within the organisation - which includes data access controls, audit trails and monitoring. Enterprises should formulate firm guidelines for how sensitive data is stored, accessed and sent so that they are aligned with regulatory expectations. This type of governance can be better facilitated through the traditional on-premises model, where there is greater control, flexibility and integration of compliance controls throughout the current IT space.

In summary, for businesses operating within strict regulatory constraints, an on-premises architecture provides a pragmatic and secure answer. This way, organizations retain full control of their data and systems, which helps them to maintain compliance requirements. On-premises governance by localizing the management and minimizing exposure to external risks and on-premises governance strengthens organizational accountability and protects sensitive information in heavily regulated industries.

4 Mitigating On-Premise IT Challenges

A study conducted by Skafi, Yunis, and Zekri (2017) indicates that when pondering the use of cloud computing, user-friendliness, superior security and privacy levels are particularly valued by IT managers and professionals. Security is especially a key concern for many, often acting as a roadblock to the adaption of cloud offerings. For example, studies conducted on cloud offerings

including Microsoft's Azure stressed how such users would always prefer to consider data security as their priority/certainty (Chang & Ramachandran, 2015). This security concentration is highly correlated with trust, notably the works of Ghazali et al. (2017), Wu (2011), Butt et al. (2019), and Mishra et al. (2020) concludes that increased sense of security leads to improved trust in the cloud technology, which makes it easier to adopt cloud technology. Cost effective is also a big motivation for the move from on-premise to cloud, with some types of cloud services, such as private clouds. It can cost a lot of money for maintenance, and service fee purchased as well (Wu et al., 2016; Changchit & Chuchuen, 2018; Chou, 2015).

However, recent research by Kalra and Moukhtar (2024) appear to indicate that it may possible to outperform cloud-based services with on-premises servers, both in raw performance and overall cost. Cloud-based platforms, such as Azure, do have scalable resources that could improve performances; however, the cost of using them is usually quite expensive. Instead, they're stuck using serverless architectures like AWS Lambda which can be lower-performance than dedicated on-premise on servers. That being said, cloud services like AWS and Azure have some very serious advantages in the ability to scale and the reliability aspects, organizations don't have nearly the amount of overhead that it does (time and money) in scaling physical infrastructure as organizations do in the cloud.

Michel (2013) also confirms the benefits of utilizing cloud by pointing out while cloud providers perform faster and cheaper services, businesses can focus more on what they do best when IT operations are outsourced to specialized cloud providers. Moving from a capital expenditure model to an operating cost model allows companies financial freedom, a point substantiated by multiple industry interviews which underscored saving money and competitive pricing as the top reasons for moving to cloud.

Clouds like Azure, allows organizations to consume computing resources just about anywhere with very little overhead in terms of administration. Minimal initial investment allows companies to take risks on new concepts and fail fast if necessary. Also, cloud scenarios allow for renegotiation of providers, even to a full decommissioning without the need of dealing with the hardware disposal.

Candidates uniformly recognize flexibility and scalability as most of the strongest advantages that cloud computing offers. Hugos and Hulitzky (2011) explains cloud computing as a disruptive combination of internet technologies, virtual servers and open sources software, which facilitates new models for the delivery of IT resources, transferring costs from fixed capital expenses to variable operating costs.

There are several benefits of cloud solutions such as in Azure, which includes the scalability, Kuumar (2023) reveals that it is an important asset, through which companies have the opportunity to flexibly adapt operational capacity based on changing demands which leads to reduction in costs and to complete business continuities. Cloud management's inherent bendiness also decreases the requirement on full-time in-house system administrators, reducing administrative overhead. In addition, cloud computing helps support remote collaboration by making it easy to securely access applications and data. It's important, though, to mention that although customers are responsible for protecting their data and apps when in the cloud, the security of the underlying infrastructure is managed by the cloud service provider. This model of shared responsibility could sometimes end up in ambiguities and dents to security if not managed rightly. And IT teams frequently have difficulties enforcing security policies and controlling access across heterogeneous cloud environments, issues that could cause them at risk of data breaches, insider attacks, compliance exceptions, and misconfigurations in the cloud. Hence, organizations need to choose cloud vendors wisely using stringent security parameters in order to alleviate those potential risks.

The energy consumption is another differentiation between on-premises and cloud data centers. Thaqi et al. (2024) demonstrate that despite potential gain in scalability and resource utilization through cloud computing, the energy behaving of on- premises data centers can be diverse depending on size, architecture, and operational routines.

Performance comparison of cloud and on-premises databases as stated by Gyorodi et al. (2018), by demonstrating that cloud options are not always better but lighter than on-premises offerings. Especially with the free-tier cloud level, response time are likely to be slower than with normal databases. However, when appropriate, higher-priced cloud tiers are employed and user loads

increase, cloud platforms tend to deliver superior performance. In most cases, the performance gaps in the two architectures are in milliseconds, so cloud computing, an elastic model with its pricing scheme that is friendly (utility, usability, expandability, reliability, security and cost-effective), in general, it is the best choice for organizations.

5 Methodology

The research methodology is developed in order to achieve the stated objectives of this research study. This chapter deals with the areas such as definition for each independent variable, theoretical scope and geographical area of the study, research design, conceptual framework, hypothesis, population and sample, instrumentation, ethical considerations and operationalization of this research study.

5.1 Definition for each Independent Variable of the Study

Performance

Computing performance pertains to a system's capacity to handle data processing and execute instructions within a specific period. It is commonly evaluated using metrics such as throughput, which indicates the volume of tasks completed per unit time, and latency, which measures the response time to a request. Achieving high performance is essential for systems that demand real-time operations or manage large volumes of data (Suthar, 2025).

Scalability

Scalability refers to a system's capacity to accommodate growing workloads by incorporating additional resources. In computing, it denotes the ability of a system to enhance its overall performance in response to increased demand, typically through the addition of hardware. This attribute is particularly important for data-intensive applications or systems undergoing rapid expansion (www.forbes.com, 2022).

Downtime

In computing, downtime signifies intervals during which a system is non-operational or inaccessible, preventing users from receiving services. Such interruptions may result from system malfunctions, scheduled maintenance, software updates, or cyberattacks. Reducing downtime is essential for maintaining service continuity and preserving user confidence (Kim, 2022).

Cost-effectiveness

Cost-effectiveness in computing refers to evaluating the expenses associated with computing resources and services in relation to the advantages and value they deliver. It plays a vital role in making informed decisions regarding the implementation of new technologies or services (www.knowledge.edu, 2021).

Security

In computing, security encompasses safeguarding systems and data against cyberattacks and identifying potential vulnerabilities that could be exploited. It involves implementing strategies and controls to prevent unauthorized access, usage, disclosure, alteration, disruption, or destruction of information. Given the rising frequency of cyber threats and the significance of data privacy, security remains a fundamental aspect of computing (www.imperva.com, 2022).

Governance/Compliance

Governance and Compliance refers to a systematic approach that ensures IT practices are aligned with business objectives while effectively managing risks and adhering to relevant industry and governmental regulations. It involves the use of tools and procedures that integrate an organization's governance, risk management, and technology adoption. This framework helps organizations achieve their goals consistently, reduce uncertainty, and fulfil compliance obligations (www.aws.amazon.com, 2025).

These factors and their respective definitions are important in the field of computing and particularly relevant when comparing different computing environments. Each of these factors plays a significant role in determining the overall effectiveness and suitability of a particular computing environment for specific applications or use-cases(Kalra and Moukhtar, 2024)

5.2 Theoretical Scope and Geographical area of the Study

The theoretical scope of this research study will be the factors of cost, security, performance, scalability, downtime/high availability and governance/compliance which are affecting for the decision for adoption of on premise or cloud computing. As per the geographical area of this research study, the IT organizations in Western province of Sri Lanka will be selected. The sample is drawn from the IT organizations in Western province of Sri Lanka which are coming under the category of IT employees between 10 to 40.

5.3 Research Design

With the consideration of present materials and methods such as international journal articles, books analysis, interviews via internet on cloud computing and on-premise computing plus conducting academic and practical discussions on cloud and on-premise computing models, the theoretical framework of the research study developed(Michel, 2013). To obtain answers for hypothesis, a non-experimental quantitative correlational research design was used(Sullivan, n.d.). As per the leveraging of collected primary data, a qualitative method was used as to measure and analyze the relationships between the variables of exogenous with the endogenous (Apuke,2017; Bacon-shone,2015).

Swanson and Holton (2005) stated that, for the generalization, as to ensure that the quantitative study is providing the best approach for the study, there must be an adequate sample size.

As to measure the effect of each factor for the decision of on premise computing adoption, a regression analysis was performed. According to the necessity of using statistical data by the study for analyzing the relationship between variable and the survey instrument, dictates the usefulness

of a quantitative method. The feasibility is there for other researchers to conduct a similar research to this and conduct a statistical comparison.

A survey instrument was used to collect data from IT leaders in enterprises across Sri Lanka especially in Western province. A well prepared structured questionnaire prepared as a Google doc. hence will be sent via an email to the sample which selected from the population with the application of simple random sampling. The intention behind reaching out to this is to capture data from IT leaders with on premise and cloud computing knowledge across the Western province in Sri Lanka.

Most of the aspects of the structured questionnaire was adapted and validated by Bani (2011). Decision making involvement in the organizations along with the on-premise and cloud computing knowledge were considered as far as the sample participants are concerned. For the participants, it is guaranteed the confidentiality and anonymity. As per the confirmation of the validity of constructs, a pilot study was conducted with the usage of reasonable few amount of respondents in advance to the main questionnaire study. Additionally, as to upgrade the findings of the research study, interviews with deep in-sight were carried out with research study's potential participants.

The ordinal scale questionnaire from 7(strongly agree) to 1(strongly disagree) with 4(neutral) has sent to the sample selected participants as a Google Form for which the participants responded to each and every question by selecting the extent to which they agreed or disagreed with the statements provided. . Additionally, they have an open-ended question to include their respective ideas/viewpoints/opinions on the concerning computer models. As per the best assessment of the relationships among various variables with the effect, the quantitative method was selected (Almeida et al., 2017). Moreover, it will leverage the statistical analysis of the study.

Cost, security, performance, scalability, down-time/high availability and governance/compliance are the independent variables and the dependent variable is decision to on premise computing adaption. To measure the strength of the relationship, Pearson's r test deployed. If it is data from a sample survey study, and if data is gathered as per the ordinal scale, an appropriate statistical tool is Pearson correlation coefficient(r) (Mukaka, 2012).

5.4 Conceptual Framework of the Study

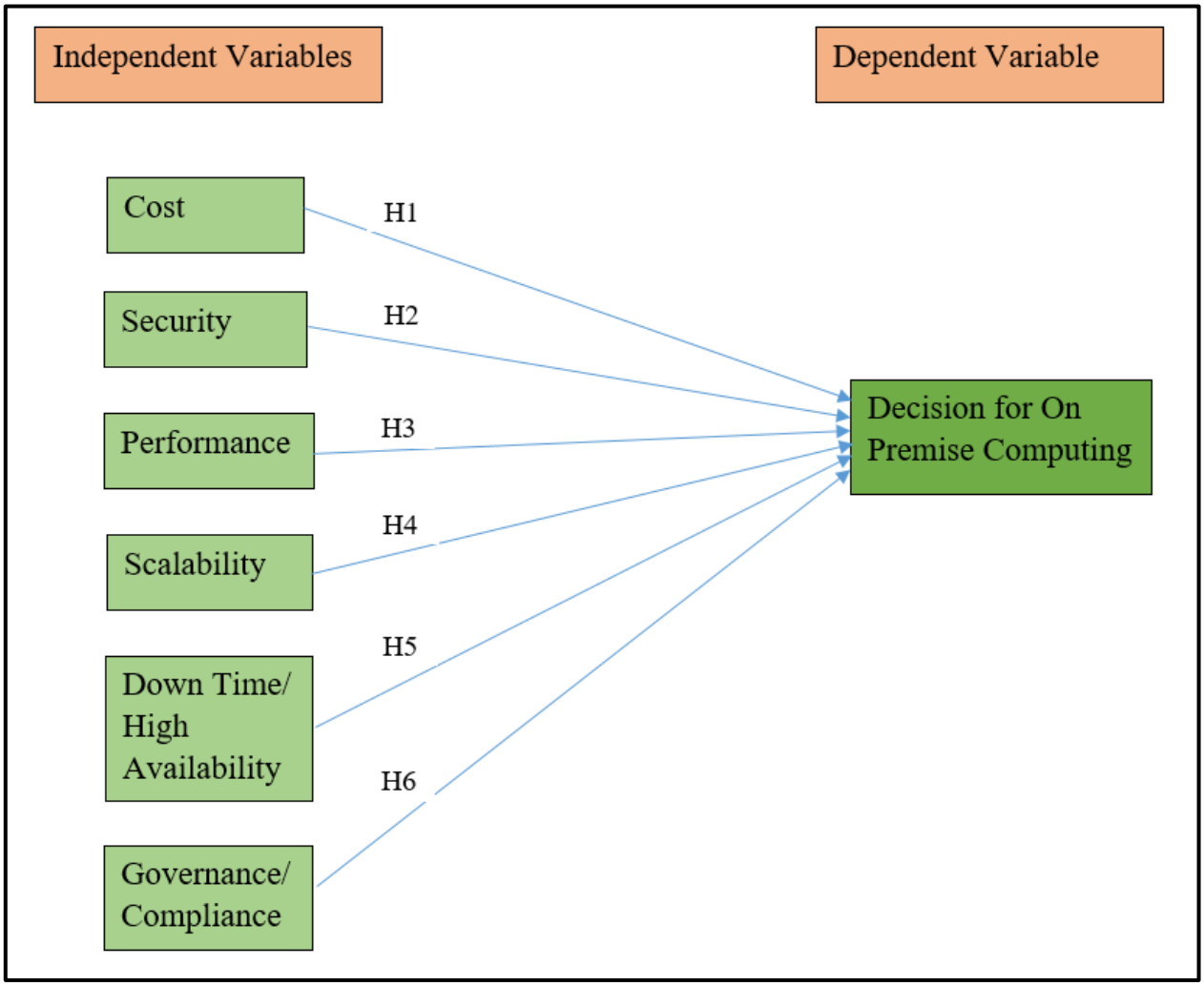

Figure 5 : Conceptual Framework

Source : Author developed based on the literature survey

- Cost: This will involve a detailed cost-benefit analysis of the hosting solutions, taking into account both direct and indirect costs (Kalra and Moukhtar, 2024).

- Security: This will involve evaluating the security measures in place to protect data and prevent unauthorized access, as well as assessing the number and severity of vulnerabilities in each hosting implementation (Kalra and Moukhtar, 2024).
- Performance: This will involve measuring the speed and responsiveness of the hosting solutions under a specific load condition (Kalra and Moukhtar, 2024).
- Scalability: This will involve assessing the ability of the hosting solutions to handle increased load without a significant drop in performance (Kalra and Moukhtar, 2024).
- Downtime/High Availability: This will involve tracking the uptime of the hosting solutions over a specified period (Kalra and Moukhtar, 2024).
- Governance/Compliance: This will involve measuring the adherence of industry and government regulations over a certain period of time (www. aws.amazon.com,2025)

5.5 Hypotheses of the Research Study

Hypotheses 1

H0: There is no significant correlation between cost and decision for on premise computing adoption in an IT organization.

H1: There is a significant correlation between cost and decision for on premise computing adoption in an IT organization.

Hypotheses 2

H0: There is no significant correlation between security and decision for on premise computing adoption in an IT organization.

H1: There is a significant correlation between security and decision for on premise computing adoption in an IT organization.

Hypotheses 3

H0: There is no significant correlation between performance and decision for on premise computing adoption in an IT organization.

H1: There is a significant correlation between performance and decision for on premise computing adoption in an IT organization.

Hypotheses 4

H0: There is no significant correlation between scalability and decision for on premise computing adoption in an IT organization.

H1: There is a significant correlation between scalability and decision for on premise computing adoption in an IT organization.

Hypotheses 5

H0: There is no significant correlation between downtime/high availability and decision for on premise computing adoption in an IT organization.

H1: There is a significant correlation between downtime/high availability and decision for on premise computing adoption in an IT organization.

Hypotheses 6

H0: There is no significant correlation between governance/compliance and decision for on premise computing adoption in an IT organization.

H1: There is a significant correlation between governance/compliance and decision for on premise computing adoption in an IT organization.

5.6 Target Population and Sample

Managers in IT organizations, IT and Technical leaders across Western province of Sri Lanka who are knowledgeable about both on-premise and cloud computing thus involve in their respective organizations' IT decisions to meet departmental or organizational goals with on-premise and/or cloud resources(Tachu, 2022) are the targeted population. The reason behind that decision is these categories of employees i.e IT and Technical leaders, IT Managers etc. are performing their duties hand-in-hand with their respective leaderships in relation to the alignment of the IT strategies with the organizational goals(McKeen & Smith, 2017; Pearlson et al., 2020).

As far as the survey's response and quality are concerned, IT and technical leaders participation impact a lot (Wright & Schwager, 2008). System administrators, network administrations, engineers etc. those who are coming under the non-leadership categories but are falling to IT Staff were also targeted as potential participants. According to Alghamdi and Bach (2018), in the process of decision making by the top management, non-management staff feedback is taken into consideration as teamwork depicts everyone. Therefore, IT staff belongs to other categories were also included.

The sampling plan will be as follows.

- **Target Population and Sample Unit** – To measure the each factor and the decision for on premise computing adoption, the unit of analysis is the IT leaders in Western province of Sri Lanka.
- **Sample size** – The total population of the IT leaders in Western province of Sri Lanka is around 5000 and Sample size is 80.
- **Sampling Method**- Simple Random Sampling is used to take the sample of 80 from the IT leaders in Western province of Sri Lanka.

The data analysis plan will be as follows.

- **Data Analysis** -As the Descriptive analysis, pie and bar charts will be used thus a regression analysis will be used as per the Multivariate analysis.

5.7 Instrumentation of the Study

Survey instruments' reliability and validity were tested by few other researchers in their other respective research efforts. Especially with other variables. The format of the survey was not altered as reliability and validity of the instrument was not compromised. Jose, Ray and Henseler (2018) have used this Bani's(2011) research instrument.

According to the Bani's (2011) research instrument, the respondents provided their responses to the seven-point Likert-scale type questionnaire. The confidence level considered is 95% by the analysis. Cleared numerical values were obtained by applying the data cleaning process to the Likert scale responses.

5.8 Ethical Considerations of the Study

It is essential to secure confidentiality and privacy of the sample participants to the survey. Accordingly, mode of anonymous is always kept in activated. The related parties those who are interested in the findings of this research study, can obtain the findings for their respective emails. The developed validated questionnaire was made comprehensively by ensuring that no any personnel or identifiable data or information is releveled pertaining to any participant to the survey. Ethical considerations and any additional recommendations are accordance with the University of JAMK. As per the achievement of the research quality, compliance and ethics pertaining to the research work are well followed along with the university guidelines. Adherence to this particular framework helped to gain sample participants trust and confidence.

5.9 Operationalization Table of the Study

Table 2: Operationalization Table of the Study

Concept	**Variables (Dimensions)**	**Indicators**	**Measures**	**Source**
	1.Cost	Power Consumption		

Main Factors (which affect for the decision of on-premise computing)	Cronbach alpha-0.791	Space Hardware requirement Software license Maintenance Storage Staff Training	7 Point-Likert scale	(Sosnovyk, 2025)
	2. Security Cronbach alpha-0.80	Data privacy Information privacy Data transfer security Firewalls VPN User authentication Physical disaster	7 Point-Likert scale	(Sosnovyk, 2025)
	3. Performance Cronbach alpha-0.72	Software/Application performance IT staff performance Hardware performance Ongoing optimization Troubleshooting	7 Point-Likert scale	(TECHVIFY ,2025)

	4. Scalability Cronbach alpha-0.698	Scaling up(horizontally and vertically) Scaling down (horizon- tally and vertically)	7 Point-Likert scale	(TECHVIFY ,2025)
	5. Downtime/High Availability Cronbach alpha-0.676	Lead time Downtime Frequency of downtime	7 Point-Likert scale	(Weaver, 2013)
	6. Governance/ Compliance Cronbach alpha-0.745	FERPA compliance HIPAA compliance	7 Point-Likert scale	(Sosnovyk, 2025)
Decision of on-premise computing	On premise com-puting Cronbach alpha-0.842	On premise computing system in operation	Nominal scale	(Sosnovyk, 2025)

6 Data Analysis

This research study was conducted on measuring the decision for On-Premise computing over the factors of cost, security, performance, scalability, downtime/high availability and governance/ compliance. Most of the experts in the IT industry participated and provided their individual answers on the questionnaire distributed via Google forms. Accordingly, 73 IT professionals reverted the

dully filled questionnaire for this research study. This sample of 73 IT professionals are belonging to more than 15 IT organizations in Western province in Sri Lanka.

6.1 Qualitative and Quantitative Analysis

6.1.1 Gender Difference of the sample

The following pie chart depicts the gender difference of the selected sample of IT professionals. Out of 73 respondents, 86.3% of the respondents are coming under the male category where 13.7% represents the female category.

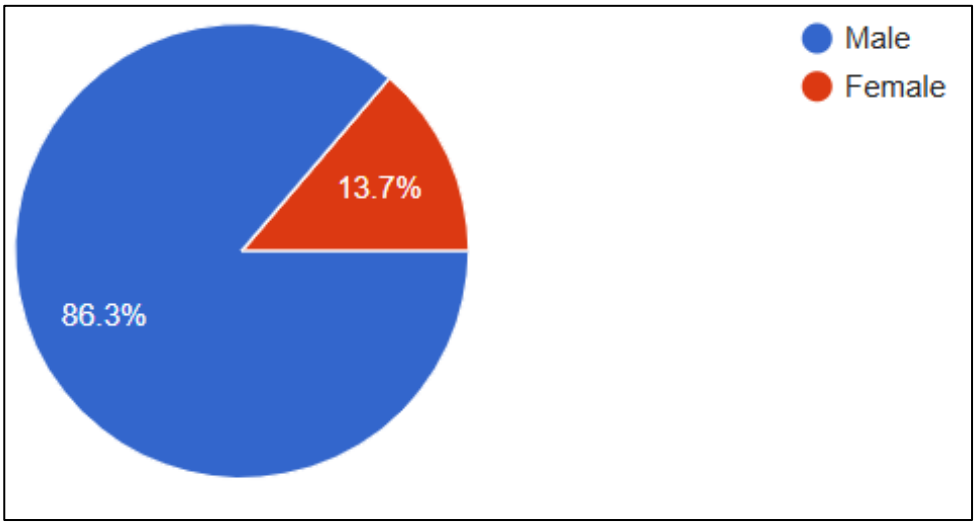

Figure 6: Gender Difference of the sample

Source: Data Analysis

6.1.2 Designation categories of the sample

As per the demographic factors of the sample, the following pie chart depicts the designation categories of the selected sample of IT professionals. Among 73 respondents, 60.3% of designations are falling under the Middle Management (Technical Leads, Team Leads etc.), 24.7% designations

are falling under the Top Management (Architects, Project Managers, Directors etc.) and the rest 5.1% designations are coming under the Bottom/Lower Management (Software Engineers, Network Engineers etc.).

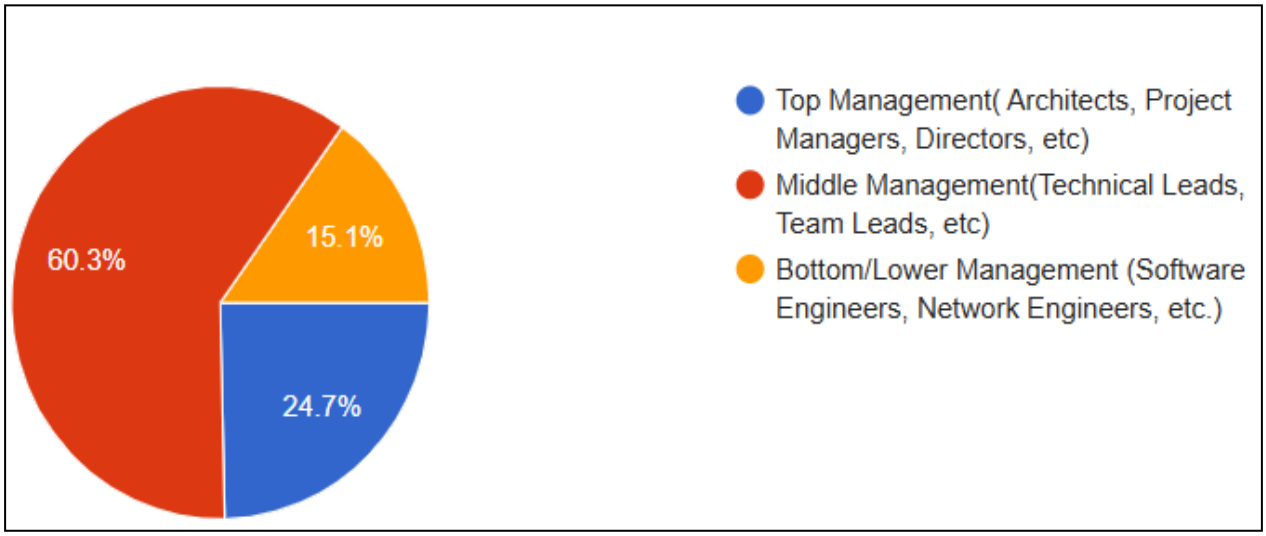

Figure 7 : Designation category of the sample

Source: Data Analysis

In the research study questionnaire, there was a question to the sample respondents to comment on their preference of On-Premises computing over Cloud computing by based on this research considering factors of cost, security, performance, downtime/high availability, scalability and governance/compliance.

The following are the comments from the sample selected IT professionals on the preference of On-Premises computing over Cloud computing.

1) Cost and performance wise on premises is better but in terms of scalability and innovation cloud is ideal.

2) Denial of wallet attacks can be a threat with the auto scaling capabilities.

3) On-premises computing always requires experts, involves extensive manual work, and demands dedicated personnel, making it very expensive.

4) Cloud server-based computing has more cons than pros relative to the Sri Lankan tele-communication bottle necks. There's latency in movements making it hard or frustrating to work, apps like teams can be very slow and networks tend to drop now and then.

5) With Cloud computing, you get flexibility, elasticity of increasing and reducing your spending base on your workload, a company with a rapid growth can really take the advantage of adapting to cloud solutions if they closely monitor and manage the instances.

6) I don't see any valid advantages of on-premises computing other than compliance and regulatory reasons.

7) Some organizations prefer on-premises computing for its greater control over data, security, and customization, while others find cloud computing more flexible and cost-effective, offering scalability and reduced maintenance.

8) While cloud computing is generally more flexible and scalable, some organizations may still prefer on-premise computing due to concerns over data security, regulatory compliance, or the need for greater control over their infrastructure. In industries with strict data governance or where legacy systems are deeply embedded, on-premise solutions can still be the preferred choice. However, the overall trend is clearly shifting toward cloud, especially with hybrid models offering a balance between both worlds.

9) When it comes to ease of use and scalability, i prefer cloud. There are special scenarios that on-premises is more suitable. The drawback of cloud is, that developers tend to ignore performance aspects due to scalability provided by cloud platforms.

10) If the organization can maintain their server farm then I still believe on-premise is a good option. Also specifically for tier1 financial application it is still not difficult to operate on cloud due their performance SLAs and security concerns. But outposts is a good solution for that.

11) Need to consider the costing as well

12) Cloud computing is more productive and easy to manage the environment. But considering the data criticality and data or application usage, better to have hybrid cloud infrastructure.

13) I think cloud computing help offload some part of responsibilities and complexity to cloud providers such as security, maintenance , fail tolerance and scaling etc which will reduce overhead over on-premise, But those thing come with higher cost.

14) Companies feel safer keeping their data in-house.

15) For regulatory reasons sometimes we have to pick on premise

16) Cloud computing preferred for all scenarios unless there's a concern on sensitive information.

17) In some cases, on premise computing is better than cloud computing. However, accessibility, availablity, extendability point of view, cloud computing is the better option.

18) Mainly the security. Sometimes cost.

19) Decision on On-Premises computing architecture depends on company's necessity.

The responses from the sample on the preference of on-premises computing over cloud computing illustrate that, the majority is using on-premise cloud solution due to data security, governance/regulatory compliance or the need for greater control over their infrastructure. By concerning other researching factors of cost, performance, scalability and downtime/high availability, according to the sample's responses, cloud computing is offering more such as saving the cost of maintenance, easy to create infrastructure, and easy to scalable the resource according to the company's needs, the company paid only the charges which the company use the web-services for short term.

6.1.3 Correlation Analysis

To study the relationship between decisions for on-premises computing, research questions were designed around the factors of cost, security, performance, scalability, downtime/high availability and governance/compliance. To obtain a granular understanding of the relationships between the dimensions and individual variables, a Pearson correlations analysis was performed for all the variables, as indicated in the table below.

Table 3: Correlation Analysis

Independent Variables		
Cost	Pearson Correlation	-.558**
	Sig. (two-tailed)	.000
	N	73
Security	Pearson Correlation	.701**
	Sig. (two-tailed)	.000
	N	73
Performance	Pearson Correlation	.572**
	Sig. (two-tailed)	.000
	N	73
Scalability	Pearson Correlation	-.344**
	Sig. (two-tailed)	.000
	N	73
Downtime/High Availability	Pearson Correlation	-.250**
	Sig. (two-tailed)	.004
	N	73
Governance/ Compliance	Pearson Correlation	.588**
	Sig. (two-tailed)	.005

	N	73

** Correlation is significant at the .01 level (two-tailed).

Source: Data Analysis

Hypotheses 1

H0: There is no significant correlation between cost and decision for on premise computing adoption in an IT organization.

H1: There is a significant correlation between cost and decision for on premise computing adoption in an IT organization.

As per the Pearson correlation analysis, the correlation value for the independent variable of cost on the dependent variable of decision for on-premises computing adoption depicted as -0.558. It clarifies that there is a significant correlation value among two variables. Because of this, the null hypothesis can be rejected, and the alternative hypothesis can be accepted. The P value is recorded as .000(P<.01) which is significant. The results indicate that there is a reasonably strong negative correlation exists(r = -0.558) between the two variables.

Hypotheses 2

H0: There is no significant correlation between security and decision for on premise computing adoption in an IT organization.

H1: There is a significant correlation between security and decision for on premise computing adoption in an IT organization.

The output of the correlation analysis in the table indicates significant correlation value for security with decision for on premise computing adoption. Therefore, the null hypothesis is rejected and the alternative hypothesis is accepted. The P value is recorded as .000(P<.01) which is significant. The results indicate that there is a strong positive correlation exists (r = 0.701). Based on the results

derived, the highest recorded correlation value is pertaining to the security and decision for on-premises computing adoption.

Hypotheses 3

H0: There is no significant correlation between performance and decision for on premise computing adoption in an IT organization.

H1: There is a significant correlation between performance and decision for on premise computing adoption in an IT organization.

According to the results of the correlation analysis, there is a significant correlation value recorded for performance on decision for on premise computing adoption. The null hypothesis can be rejected and the alternative hypothesis can be accepted. The P value recorded is .000(P<.01) which is significant. The output of results showcase that the is a strong positive correlation(r = 0.572).

Hypotheses 4

H0: There is no significant correlation between scalability and decision for on premise computing adoption in an IT organization.

H1: There is a significant correlation between scalability and decision for on premise computing adoption in an IT organization.

The correlation analysis results in the table indicates a negative correlation value for scalability on decision for on premise computing adoption. The null hypothesis can be rejected and the alternative hypothesis can be accepted. The P value recorded as .000(P<.01) which is significant. The results indicate that there is a weak negative correlation exists(r = -0.344).

Hypotheses 5

H0: There is no significant correlation between downtime/high availability and decision for on premise computing adoption in an IT organization.

H1: There is a significant correlation between downtime/high availability and decision for on premise computing adoption in an IT organization.

As of the correlation analysis results, a negative correlation value depicts in between downtime/high availability and decision for on premise computing adoption in an IT organization. Hence, the null hypothesis is rejected and the alternative hypothesis is accepted. The P value recorded as .004(P<.01) which is significant. A weak negative correlation (r = -0.250) can be identified between downtime/high availability and decision for on premise computing adoption according to the results.

Hypotheses 6

H0: There is no significant correlation between governance/compliance and decision for on premise computing adoption in an IT organization.

H1: There is a significant correlation between governance/compliance and decision for on premise computing adoption in an IT organization.

A Pearson correlation analysis of the variables illustrates that there is a significant correlation value between governance/compliance and decision for on premise computing adoption. Consequently, the null hypothesis is rejected and the alternative hypothesis is accepted. The P value is .005(P<0.01). The results demonstrates that there is a strong positive correlation(r = 0.588).

6.1.4 Regression Analysis

A regression analysis was performed as to explore the effect of each independent variable(cost, security, performance, scalability, downtime/ high availability and governance/compliance) to the dependent variable of decision for on premise computing. Given that the data was captured using an ordinal scale. The linear regression analysis was taken as:

Table 4: The regression output

On-Pre Dcn	Coef.	P- Value
cost	-.502381	0.059
secu	.612229	0.092
perf	.526630	0.074
Scal	-.445234	0.086
Down	-.376234	0.052
GoCo	.586534	0.066

R squire = 0.5682

(Source: Data Analysis)

Mean_On-Pre Dcn = intercept + B1 * cost + B2 * security + error

The regression equation is,

On-Pre Dcn = 0.1385 - 0.5023 * cost + 0.6122 * security + 0.5266 * performance - 0.4452 * scalability - 0.3762 * downtime + 0.5865 * gover-compli + error

The R squire value of 0.5682 illustrates that the overall model is well fit the data where a 56% of the total variation of decision on On-Premise (dependent variable) can be jointly explained by the independent variables of cost, security, performance, scalability, downtime and governance/ compliance.

Constant value of the regression model is 0.1385. It indicates, when all the independent variables of cost, security, performance, scalability, downtime and governance/ compliance equal to 0, the dependent variable (Decision for On-Premise Computing) carries the value of 0.1385.

The Beta value of Cost is 0.5023. It depicts that Decision for On-Premise Computing changes from 0.5023 units for 1 unit of Cost change when all the other independent variables are remain constant.

The Beta value of Security is 0.6122. It shows that Decision for On-Premise Computing changes from 0.6122 units for 1 unit of Security change when all the other independent variables are remain constant.

The Beta value of Performance is 0.5266. It identifies that Decision for On-Premise Computing changes from 0.5266 units for 1 unit of Performance change when all the other independent variables are remain constant.

The Beta value of Scalability is 0.4452. It demonstrates that Decision for On-Premise Computing changes from 0.4452 units for 1 unit of Scalability change when all the other independent variables are remain constant.

The Beta value of Downtime/High Availability is 0.3762. It displays that Decision for On-Premise Computing changes from 0.3762 units for 1 unit of Downtime/High Availability change when all the other independent variables are remain constant.

The Beta value of Governance and Compliance is 0.5865. It displays that Decision for On-Premise Computing changes from 0.5865 units for 1 unit of Governance and Compliance change when all the other independent variables are remain constant.

As far as the relationships of each independent variable to the dependent variable is concerned, the independent variables of Cost, Scalability and Down Time/High Availability recorded a negative(-) relationship with the dependent variable of Decision for On-Premise Computing.

Meanwhile, the independent variables of Security, Performance and Governance & Compliance are recorded a positive(+) relationship with the dependent variable of Decision for On-Premise Computing.

6.2 Reliability and Ethicality of the Research Results

It is very vital to discuss the reliability of the results generated from the research study. For this research study, the researcher referred a great deal of previous scholarly work in relation to many

scholars all over the world. Very especially, the researcher practically observed the real image of the research gap which is identified from both the aspects of practical observation over the years plus previous scholarly work. Once the identified gap is clearly defined, the research questions and objectives developed as to address the identified research gap.

The conceptual model was developed comprehensively by including all the independent variables and dependent variable to the research study which were clearly identified through the wider reference of existing research knowledge sources. Very importantly, the conceptual model was developed to achieve the stated research objectives which directly answers the stated research questions. The questionnaire was developed and validated appropriately for which all the anonymous sample participants answered independently and confidentially. As per the analysis, the researcher used the raw data from the participants without any alteration which ensures the real picture is depicted through the data analysis and results. Futhermore at the data collection period, participants' data collected anonymously and privacy. Besides, the conclusion and the recommendations provided are solely based on the research findings of this research where any interested party can utilize every single important point within this research effort for their future efforts in relation to research or practical business issues. Moreover, the researcher strictly followed the guidelines and ethical considerations of the University in relation to a research effort. Therefore, all these measures were undertaken by the researcher as to ensure reliability, ethicality, relevance, transparency and validity of the research.

7 Results

The purpose of this non-experimental quantitative correlational study was to identify the main factors driving organizations to prefer on-premise IT systems over cloud-based solutions in Sri Lanka IT companies, execution of a comprehensive comparison on identified factor in relation to On Premise Computing and Cloud Computing in IT organizations followed by providing recommendations to correctly address and mitigate the impact of the most influential factor for the preference of on-premise computing. Accordingly, cost, security, performance, downtime/high

availability, scalability, governance/compliance were identified as main factors affecting for the decision of on-premise computing.

In the comparison between on-premise computing and cloud computing across various identified factors, on-premises systems require the setup and configuration of hardware, software, and infrastructure, which must be continuously maintained, monitored, and troubleshooted in the event of issues. Scaling such systems is both expensive and time-consuming, as it involves the manual purchase and installation of additional memory or storage components. In terms of security, on-premises solutions are considered less risky since data is stored internally and not transmitted over the internet. Conversely, cloud computing offers cost-effective storage and on-demand computational resources, significantly reducing complexity and long deployment times, which has impacted the continued use and adoption of traditional on-premises technologies. Additionally, cloud computing supports independent scalability across computing, storage, and services. It also contributes to modern advancements in business intelligence by enabling organizations to adapt rapidly to external changes and embrace new trends, with performance improving over time.

According to the correlation analysis, it indicated positive relationships by the independent variables of security, performance, governance/compliance with the dependent variable of decision for on-premise computing where the independent variables of cost, scalability and downtime/high availability recorded a negative relationship with the dependent variable of decision for on-premise computing. By based on the statistical analysis performed with the usage of raw data collected from the selected sample, the factor of ‘security’ was identified as the most influential factor on the decision of on-premise computing adaptation. As far as the recommendations for mitigating the impact of most influential factor which is security for the decision of undertaking on-premise computing.

8 Conclusion

8.1 Meeting the Goals

Basically the research study set three major questions under the 'Research Questions of the Study' sub-heading of Introduction chapter. As per the first question, which is identification of the main factors driving organizations to prefer on-premise computing over cloud computing in Sri Lanka's IT companies, the factors such as cost, security, performance, downtime/high availability, scalability, governance/compliance were identified.

The second research question encourages the researcher to compare on-premise computing and cloud computing, referring to relevant reviewed academic literature from international scholars and the present business knowledge and experience. Cloud computing provides a relatively low-cost storage and on-demand computing capacity so as to alleviate the complexity and latency in system deployment. This has been preventing the ongoing use and effectiveness of legacy on-premise systems. Besides, cloud computing allows independent scalability of computing, storage and services. In contrast, on-premise computing necessitates the configuration of hardware, software, and infrastructure, all of which require ongoing implementation, monitoring, and issue resolution. Scaling such systems is both costly and time-intensive, as it involves manually acquiring and configuring additional memory and storage. In terms of security, on-premise solutions present minimal risk since data is stored internally and not transmitted over the internet.

The third research question which is to provide recommendations to address and mitigate the impact of the most influential factor which drives the preference for on-site IT systems in Sri Lanka IT companies, the results recognized most influential factor is 'security' where the IT companies have select the right cloud architecture which ensures the highest security, storing sensitive data in secured private cloud, selecting cloud service providers which are certified under the government level security standards and compliance are very crucial.

9 Recommendation

The research findings confirmed, ‘security’ is the most prominent factor on the decision for on premise computing adaptation. It can be recommended that, if the IT organization is going to undertake the correct cloud computing system in a correct manner, ensuring the highest rate of ‘security’ is guaranteed from the cloud computing service provider. For that, the IT organization itself must select the right cloud architecture, adhere to the robust security controls and need to maintain compliance with industry-specific regulations. Leading cloud service providers concurrently provide ‘sovereign cloud’ options where data never leaves the country or a specific region. i.e. Azure Confidential Computing etc. Many providers are certified for government level security standards hence ensure compliance with GDPR, HIPAA, FISMA, FedRAMP, PCI-DSS, etc. moreover, provide confidential computing(end-to-end encryption)) to encrypt data even during processing. This type of confidential computing prevents cloud admins or malicious insiders from accessing sensitive data. In addition, sensitive data can be stored in private cloud which is highly secured. With an ideal cloud computing system, it can be implemented IAM with zero trust architecture. Enabling detailed auditing, logging, and forensic tracking plus integrating with HSMs for encryption key protection are also possible avenues to ensure more security in a cloud computing system. As to ensure high security of the connectivity, cloud computing adopted IT organization can use private networks (VPN, Direct Connect, ExpressRoute) instead of public internet, under custom security policy endorsement.

9.1 Future Research Avenues

Since the geographical scope of the research study was limited to the western province in Sri Lanka, a future research effort can aim at world-wide geographical scope where such a research effort can obtain data from a sample across the world. In addition, future research efforts can focus on different industries plus different sizes of the companies for research efforts. Future research efforts with more deep statistical analysis on the factors with more data fill-ups, will also be highly productive.

References

A, K., & Y, M. (2024). *ESSAYS.SE: Comparative Analysis of On-Premises and Cloud Hosting Solutions*. Essays.se. https://www.essays.se/essay/7cff15a759/

Abdulmajeed, A & Christian, B., (2018). Developing Teamwork at Workplace. International Journal of Business and Management Invention, Vol. 7, Issue. 2, February 2018. 28-40.

Adaptive Network Access & Security Solutions | NordLayer. (n.d.). Nordlayer.com. Retrieved December 11, 2021, from https://nordlayer.com/

Almeida, Fernando & Faria, Daniel & Queirós, André. (2017). Strengths and Limitations of Qualitative and Quantitative Research Methods. European Journal of Education Studies. Vol. 3, 369-387. 10.5281/zenodo.887089.

Al-Sharafi, M. A., Arshah, R. A., & Abu-Shanab, E. A. (2017). Factors Influencing the Continuous Use of Cloud Computing Services in Organization Level. *Proceedings of the International Conference on Advances in Image Processing*. https://doi.org/10.1145/3133264.3133298

Alkhater, N., Walters, R., & Wills, G. (2018). An empirical study of factors influencing cloud adoption among private sector organisations. *Telematics and Informatics*, *35*(1), 38–54. https://doi.org/10.1016/j.tele.2017.09.017

Alshamaila, Y., Papagiannidis, S., & Li, F. (2013). Cloud computing adoption by SMEs in the north east of England. *Journal of Enterprise Information Management*, *26*(3), 250–275. https://doi.org/10.1108/17410391311325225

Apuke, O. D. (2017). Quantitative research methods : A synopsis approach. *Kuwait Chapter of Arabian Journal of Business and Management Review*, *6*(10), 40–47. ResearchGate. https://doi.org/10.12816/0040336

Armbrust, M., Stoica, I., Zaharia, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., & Rabkin, A. (2010). A View of Cloud Computing. *Communications of the ACM*, *53*(4), 50–58. https://doi.org/10.1145/1721654.1721672

Avram, M. G. (2018). Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective. *Procedia Technology*, *12*(12), 529–534. Science Direct. https://doi.org/10.1016/j.protcy.2013.12.525

Bani-Ahmad, (2017). Bani-Ahmad. "X-Pro Milestone: Comparative Evaluation against Similar Software Tools, Current Status, and Planned Future Directions". Creative Education (CE). Vol.8 No.4, April 2017. Pages 627-649. doi: 10.4236/ce.2017.84048. https://sites.google.com/site/theexprosite/

Benitez, J., Ray, G., & Henseler, J. (2018). Impact of information technology infrastructure flexibility on mergers and acquisitions. MIS Quarterly: Management Information Systems, Vol.42, No.1, 25-43. https://doi.org/10.25300/MISQ/2018/13245).

Chang, V., & Ramachandran, M. (2016). Towards Achieving Data Security with the Cloud Computing Adoption Framework. *IEEE Transactions on Services Computing*, *9*(1), 138–151. https://doi.org/10.1109/tsc.2015.2491281

Collidu. (2022, May 11). *Cloud Cost Management*. Collidu.com. https://www.collidu.com/presentation-cloud-cost-management

Correia, S. R. V., & Martens, C. D. P. (2022). Cloud computing projects: critical success factors. *RAUSP Management Journal*, *58*(1). https://doi.org/10.1108/rausp-06-2021-0107

Dempsey, D., & Kelliher, F. (2017). Cloud Computing. *Industry Trends in Cloud Computing*, 9–28. https://doi.org/10.1007/978-3-319-63994-9_2

Endicott, P. (2019). Novacene; the coming age of hyperintelligence. *Medicine, Conflict and Survival*, *35*(3), 284–286. https://doi.org/10.1080/13623699.2019.1662893

Fisher, C. (2018). Cloud versus On-Premise Computing. *American Journal of Industrial and Business Management*, *08*(09), 1991–2006. https://doi.org/10.4236/ajibm.2018.89133

FS. (2024). *Fibre Optic Transceiver Module & Cable Solutions - FS.com Europe*. FS.com. https://www.fs.com/

Ghosh, S. K., Lee, J., Godwin, A. C., Oke, A., Reem Al-Rawi, & Mervat El-Hoz. (2016). *Waste management in USA through case studies: e-waste recycling and waste energy plant. 894362*.

Groom, F. M., & Jones, S. S. (2018). Enterprise Cloud Computing for Non-Engineers. In *Auerbach Publications eBooks*. https://doi.org/10.1201/9781351049221

Ho, D. (2023, September 28). *On-premises Vs Cloud: A Clear Comparison - Techvify*. Techvify. https://techvify.com/on-premises-vs-cloud-a-clear-comparison/

Hugos, Michael , Hulitzky, & Derek. (2011). Business in the cloud: what every business needs to know about cloud computing. *Choice Reviews Online*, *48*(08), 48–457448–4574. https://doi.org/10.5860/choice.48-4574

Injadat, M., Moubayed, A., Nassif, A. B., & Shami, A. (2021). Machine learning towards intelligent systems: applications, challenges, and opportunities. *Artificial Intelligence Review*, *54*. https://doi.org/10.1007/s10462-020-09948-w

Isom, P. K., & Holley, K. (2012). *Is Your Company Ready for Cloud*. IBM Press.

Izraylevych, I., & Sosnovyk, D. (2022, July 6). *Cloud Computing vs. On-Premises: Advantages, Disadvantages, and Cost Comparison*. S-pro Blog. https://s-pro.io/blog/cloud-computing-vs-on-premises-advantages-disadvantages-and-cost-comparison

Kim, Hanjun , Pendergrass, Angeline, & Kang. (2022). The dependence of mean climate state on shortwave absorption by water vapor. *Journal of Climate*, 1–54. https://doi.org/10.1175/jcli-d-21-0417.1

Kumar, G., Kapil Kumar Goyal, & Batra, N. (2019). Evolution, principles and recent trends in reconfigurable manufacturing system. *Journal of Physics*, *1240*(1), 012161–012161. https://doi.org/10.1088/1742-6596/1240/1/012161

Kushwaha, A. (2020). AWS Cloud Infrastructure vs Traditional On-Premise. *International Research Journal of Engineering Technology*, *pp.*(175–180, 2020). www.irjet.net.

Laghari, A. A., He, H., Shafiq, M., & Khan, A. (2018). Assessment of quality of experience (QoE) of image compression in social cloud computing. *Multiagent and Grid Systems*, *14*(2), 125–143. https://doi.org/10.3233/mgs-180284

LeeSangjae, & KimKyoung-jae. (2007). Factors affecting the implementation success of Internet-based information systems. *Computers in Human Behavior*. https://doi.org/10.5555/1224812.1225108

Lian, J.-W., Yen, D. C., & Wang, Y.-T. (2014). An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. *International Journal of Information Management*, *34*(1), 28–36. https://doi.org/10.1016/j.ijinfomgt.2013.09.004

McKeen, J. D., & Smith, H. (2003). *Making IT Happen: Critical Issues in IT Management*.

Microsoft Azure. (n.d.). *Cloud Computing Services | Microsoft Azure*. Azure.microsoft.com. https://azure.microsoft.com/en-us

Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security*, *120*(1), 102820. sciencedirect. https://doi.org/10.1016/j.cose.2022.102820

Misra, S. C., & Mondal, A. (2011). Identification of a company's suitability for the adoption of cloud computing and modelling its corresponding Return on Investment. *Mathematical and Computer Modelling*, *53*(3), 504–521. https://doi.org/10.1016/j.mcm.2010.03.037

Muhammad Shiraz, Saeid Abolfazli, Zohreh Sanaei, & Gani, A. (2013). A study on virtual machine deployment for application outsourcing in mobile cloud computing. *The Journal of Supercomputing*, *63*(3), 946–964. https://doi.org/10.1007/s11227-012-0846-y

Mukaka, M., (2012). A Guide to Appropriate Use of Correlation Coefficient in Medical Research. Malawi Medical Journal, Vol. 24, Issue 3, September 2012, 69-71.

Nazir, S., Khan, S., Khan, H. U., Ali, S., Garcia-Magarino, I., Atan, R. B., & Nawaz, M. (2020). A Comprehensive Analysis of Healthcare Big Data Management, Analytics and Scientific Programming. *IEEE Access*, *8*, 95714–95733. https://doi.org/10.1109/access.2020.2995572

Nikita, K. S. (2025). Editorial 2024 Reflections and Perspectives for the Year Ahead. *IEEE Transactions on Antennas and Propagation*, *73*(1), 4–6. https://doi.org/10.1109/tap.2025.3527376

Olumide Olufowote, J. (2017). Symbolic Convergence Theory. *The International Encyclopedia of Organizational Communication*, 1–8. https://doi.org/10.1002/9781118955567.wbieoc202

On Hybrid Cloud. Interview with Mathias Golombek. | ODBMS Industry Watch. (2025). Odbms.org. https://www.odbms.org/blog/2025/02/on-hybrid-cloud-interview-with-mathias-golombek/

On Premise Vs Cloud: 6 Key Differences Between On Premise and Cloud. (2019, May 9). Folio3 Dynamics Blog. https://dynamics.folio3.com/blog/on-premise-vs-cloud-erp-software-difference/

Rossitto, C., Ciolfi, L., Martin, D., & Conein, B. (Eds.). (2014). *COOP 2014 - Proceedings of the 11th International Conference on the Design of Cooperative Systems, 27-30 May 2014, Nice (France)*. Springer International Publishing. https://doi.org/10.1007/978-3-319-06498-7

Skafi, M., Yunis, M., & Zekri, A. (2020). Factors Influencing SMEs' Adoption of Cloud Computing Services in Lebanon: An Empirical Analysis Using TOE and Contextual Theory. *IEEE Access*, *8*, 1–1. https://doi.org/10.1109/access.2020.2987331

Skilton, P. F., & Dooley, K. J. (2010). The Effects of Repeat Collaboration on Creative Abrasion. *Academy of Management Review*, *35*(1), 118–134. https://doi.org/10.5465/amr.35.1.zok118

Stam, J. (2009). *Nucleus: Towards a unified dynamics solver for computer graphics*. https://doi.org/10.1109/cadcg.2009.5246818

Suthar, B., Zubair, M., & Jung, S. (2025). Self-folding Gravity Compensation Mechanism for a Supplementary Folding Robot Arm: Design, Analysis and Implementation. *Robotics and Autonomous Systems*, 104984–104984. https://doi.org/10.1016/j.robot.2025.104984

Swanson, R.A. and Holton III, E.F. (2005) Research in Organizations: Foundations and Methods of Inquiry. Berrett-Koehler Publishers, Inc., San Francisco, CA. Journal of Human Resource and Sustainability Studies, Vol.7 No.2, June 28, 2019.

Szabolcs Rozsnyai, Slominski, A., & Doğanata, Y. N. (2011). *Large-Scale Distributed Storage System for Business Provenance*. https://doi.org/10.1109/cloud.2011.28

Tachu, E., (2022). A Quantitative Study of the Relationship between Cloud Flexibility and On-Premise Flexibility. Issues in Information Systems, Vol.23, Issue 1, 2022, 214-238.

Weaver, Kim, Metzer, & Szendrey. (2013). THE IMPACT OF VIDEO GAMES ON STUDENT GPA, STUDY HABITS, AND TIME MANAGEMENT SKILLS: WHATS THE BIG DEAL? *Issues in Information Systems*, *Vol.14*(No.1, 122-128.). https://doi.org/10.48009/1_iis_2013_122-128

Wright, B., & Schwager, P. H. (2008). Online Survey Research: Can Response Factors Be Improved? *Journal of Internet Commerce*, *7*(2), 253–269. https://doi.org/10.1080/15332860802067730

Younus, M., Nurmandi, A., Mutiarin, D., Luhur Prianto, A., Abdul Manaf, H., & Irawan, B. (2024). Running Digital Political Marketing Movement for Election 2024: A Case Study of Pakistan. *Journal of Political Marketing*, 1–23. https://doi.org/10.1080/15377857.2024.2438379

Appendices

Appendix 1. Questionnaire

Research Topic:

Main Factors Influencing Companies to Advocate for Traditional On Premise IT Systems in the Era of Cloud Technology Dominance

Questionnaire

Part 01

You can write down the answers in the blanks or put a tick mark (✓) to indicate either 'Agree' or 'Disagree' in the box given with the questions.

1) Gender: ☐ Female ☐ Male

2) Your position in the organization is coming under which category:

Top Management ☐
Middle Management ☐
Bottom/Lower Management ☐

3) Other Comments(preference of on premise computing over cloud computing):

……
……
……
……
……
……
……

Part 02

Circle the most appropriate answer for the statement

Q. no	Statement	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neutral (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree(7)
1. Cost reduction through the adoption of On Premise Computing								
1	The organization focuses on modern IT system projects which aim to reduce cost	1	2	3	4	5	6	7
2	On premise reduces cost by executing operations and services through it	1	2	3	4	5	6	7
3	The services of on premise computing in the organization are less expensive than cloud computing	1	2	3	4	5	6	7
4	On premise computing offer free services to the organization	1	2	3	4	5	6	7
5	On premise computing helps to reduce other expenses than cloud	1	2	3	4	5	6	7
6	On premise provides innovative institution services without increasing the cost or the price of the service	1	2	3	4	5	6	7
2)	**Security Effectiveness**							
1	The data security is the biggest requirement in the organization	1	2	3	4	5	6	7
2	The strength of the data security is high in on premise computing compared to cloud computing	1	2	3	4	5	6	7
3	There is more confidence regarding on premise computing over cloud computing	1	2	3	4	5	6	7
4	The adoption and use of on premise computing lead to develop a plan to protect the security and confidentiality of the information	1	2	3	4	5	6	7
5	The confidence increases with the on premise computing over hacking, pirating and electronic security breaches	1	2	3	4	5	6	7

	3) Performance							
1	On premise computing helps on the development of innovation in the organization	1	2	3	4	5	6	7
2	On premise computing helps on the increment of the efficiency of IT staff in the organization	1	2	3	4	5	6	7
3	On premise computing facilitates to obtain better profit for the organization for its business operations	1	2	3	4	5	6	7
4	On premise computing contributes efficiently for the better achievement of other organizational objectives	1	2	3	4	5	6	7
5	On premise computing allows organization to offer satisfactory service/s to its existing and potential customers	1	2	3	4	5	6	7
4)	**Scalability**							
1	It's a huge challenge for the organization to scale-up the on premise server frequently	1	2	3	4	5	6	7
2	When scaling-up or down, the organization requires significant lead times and downtimes	1	2	3	4	5	6	7
3	When scaling-up or down, the organization requires current system to go 'offline'	1	2	3	4	5	6	7
4	Its difficult to constantly match changing infrastructure needs to physical hardware resources	1	2	3	4	5	6	7
5) Downtime/ High Availability								
1	The downtime is the biggest challenge facing by the organization when adopting on premise computing	1	2	3	4	5	6	7
2	The adoption and use of on premise computing lead to develop a plan to face the downtime occurs through it	1	2	3	4	5	6	7
3	Though there is a downtime, it's highly safer to continue with on premise computing than cloud computing	1	2	3	4	5	6	7
6)	**Governance/Compliance**							
1	The organization has taken enough efforts to ensure compliance with all applicable regulations i.e. FERPA, HIPAA	1	2	3	4	5	6	7

2	The organization is ever-ready to answer any breach of such laws	1	2	3	4	5	6	7
3	Being compliant with all the laws and regulations, the organization is achieved a better management and control	1	2	3	4	5	6	7