ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

CHALLENGES OF LOCAL CLOUD SERVICE PROVIDERS AND BANKING SECTOR IN ETHIOPIA

By: Meaza Markos

ID: GSE/0790/14

January, 2025

ADDIS ABABA, ETHIOPI

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

CHALLENGES OF LOCAL CLOUD SERVICE PROVIDERS AND BANKING SECTOR IN ETHIOPIA

A Thesis Submitted to School of Graduate Studies of Addis Ababa University in Partial Fulfillment of the Requirements for the Degree of Master of Science in Information Systems

By: Meaza Markos

Advisor: Dereje Teferi (Ph.d.)

January, 2025

ADDIS ABABA, ETHIOPIA

Declaration

This thesis has not previously been accepted for any degree and is not being concurrently submitted in candidature for any degree in any university. I declare that the thesis is a result of my own investigation, except where otherwise stated. I have undertaken the study independently with the guidance and support of my research advisor. Other sources are acknowledged by citations giving explicit references. A list of references is appended.

Signature: _____

Meaza Markos

This thesis has been submitted for examination with my approval as university advisor.

Advisor's Signature: _____

Dereje Teferi (Ph.D.)

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

CHALLENGES OF LOCAL CLOUD SERVICE PROVIDERS AND BANKING SECTOR IN ETHIOPIA

BY

MEAZA MARKOS

NAME AND SIGNATURE OF MEMBERS OF THE EXAMINING BOARD

Name	**Signature**	**Date**
Dereje Teferi (PhD) Advisor	----------	----------
Getachew H/Mariam (PhD) Examiner	----------	----------
Lemma Lessa (PhD) Examiner	----------	----------

Acknowledgement

First and foremost, I would like to express my deepest gratitude to **God Almighty** for granting me the strength, wisdom, and perseverance to complete this thesis. Without His guidance and blessings, this work would not have been possible.

I am profoundly grateful to my advisor, Dr. Dereje Teferi for his invaluable support, guidance, and encouragement throughout this journey. Your expertise and constructive feedback have been instrumental in shaping this thesis, and I am truly fortunate to have had the opportunity to learn under your mentorship.

I would also like to extend my heartfelt thanks to my family for their unwavering love, patience, and encouragement. Your constant support has been my greatest source of strength, and I am forever grateful for your belief in me.

Lastly, I would like to acknowledge my classmates, whose companionship, collaboration, and mutual support have made this academic journey an enriching and memorable experience. Thank you for your kindness and for inspiring me to give my best.

To all who have contributed to the completion of this work, directly or indirectly, my sincerest thanks and appreciation.

Abstract

Cloud computing offers transformative benefits for banks, including cost savings, scalability, improved data management, and enhanced flexibility. Despite the availability of local cloud service providers in Ethiopia, banks continue to invest heavily in building expensive data centers and IT infrastructures, which could otherwise be managed through cloud services. This study investigates the challenges and benefits of adopting cloud computing in the Ethiopian banking sector and explores the challenges faced by local cloud service providers in offering services to banks.

Employing a qualitative research approach with a case study design, the study utilized the TOE framework and insights from existing literature to guide data collection and analysis. Data was gathered through semi-structured interviews with representatives from selected banks, local cloud providers, and governing bodies. Thematic analysis was used to identify key findings across technological, organizational, and environmental dimensions.

The study revealed critical challenges and benefits for banks and local cloud providers in areas such as security and data protection, service availability and reliability, cybercrime, integration with legacy systems, limited flexibility, data recovery, vendor lock-in, and cost management. From the governing body's perspective, the lack of comprehensive regulations, standards, and frameworks to govern local cloud services was evident, with gaps identified in regulatory compliance, data sovereignty and residency, cybersecurity and data protection standards, risk management, auditing mechanisms.

The study concluded that while local cloud computing services can significantly enhance the efficiency and competitiveness of Ethiopian banks, the absence of clear regulatory frameworks and standards poses significant barriers. Addressing these gaps through coordinated efforts by governing bodies, banks, and cloud service providers is crucial to unlocking the full potential of cloud computing in Ethiopia. This alignment enables banks to transition from costly, in-house data center models to more agile and cost-effective cloud-based solutions residing in Ethiopia, fostering growth and innovation in the sector.

Keywords: TOE framework, Local Cloud Computing Service

Table of Contents

List of Tables

List of Figures

List of Acronyms

AACTS	Alta-Africom Cloud Technology Services
CC	Cloud Computing
DOI	Diffusion of Innovation
ETB	Ethiopian Birr
GUI	Graphical User Interface
IT	Information Technology
INSA	Information Network security Agency
IDC	International Data Corporation
NBE	National Bank of Ethiopia
NIST CSF	National Institute of Standards and Technology
SLA	Service level Agreements
SOC	Operations Center
SOC	Security Operations Center
TOE	Technology-Organization-Environment
TOE	Technology-Organization-Environment
TAM	Technology Acceptance Model
UTAUT	Unified Theory of Acceptance and Use of Technology
VPN	Virtual Private Networks

CHAPTER ONE

INTRODUCTION

Cloud computing is a technology that allows you to access and use computing resources like storage, processing, and networking over the internet without the need to manage or own them. Instead of buying and maintaining your own physical servers and data centers, consider cloud computing as renting a virtual pool of shared resources from a service provider.

Cloud computing has evolved as a disruptive technology that changes the way businesses handle and process data, allowing for greater scalability and flexibility in information systems. In today's dynamic business climate, where demands and workloads fluctuate, cloud computing provides a strong alternative to fulfill the changing needs of companies. It refers to the internet-based delivery of computing resources such servers, storage, databases, and software applications. It gives companies access to a shared pool of configurable computer resources that can be quickly deployed and released with little administration work. This cloud-based infrastructure provides substantial benefits in terms of scalability and flexibility for information systems (Amenwerth, 2023).

The adoption of cloud computing has far-reaching ramifications for information systems. It improves cost effectiveness by eliminating the need for substantial initial infrastructure investments and lowering maintenance and operating costs. Cloud-based solutions promote collaboration and remote work by giving anytime, anywhere access to apps and data, allowing geographically dispersed teams to work efficiently together. Furthermore, cloud computing improves data security by implementing strong security mechanisms like encryption, access limits, and frequent security updates. Cloud service providers frequently invest extensively in security systems, providing greater levels of protection than many enterprises can manage on their own (Joe, 2023).

In today's world, technology plays an increasingly important role in the banking business. In this sense, cloud computing is an emerging concept that is rapidly gaining popularity in the financial sector. This is owing to the fact that it provides banks with a variety of benefits, including online data storage (Dennis & Ravi, 2019).

According to the National Institute of Standards and Technology (NIST). Cloud Computing is "A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications, and services that can be

rapidly provisioned and released with minimal management effort or service provider interaction " (Laghari et al., 2018).

1.1 Background

For more than a decade, information technology has been rapidly evolving and has had a significant impact on almost every aspect of daily life. Businesses are facing new challenges as a result of the rapidly increasing digitalization and digitization of their environments. Cloud computing is a key technology driver in this progress. It has a significant impact on organizational digitization and necessitates changes in enterprises' information technology (IT) departments.

Traditionally, banks used on-premises IT infrastructure to handle core banking functions such as data storage, transaction processing, customer relationship management, and regulatory compliance. However, the limits of traditional infrastructure, such as high prices, restricted scalability, and complex maintenance requirements, have encouraged banks to look for new alternatives to meet these issues efficiently.

Cloud computing is making an impact in nearly every business area around the world, and the banking industry does not want to be left behind. Cloud computing is a cutting-edge IT technology that enables individuals and organizations to use the internet to access powerful hardware, software, and tools. The resources from which they can use these services are usually powerful and sophisticated computers placed in faraway locations for security purposes (Achuthan, 2019).

Cloud computing has enormous potential for revolutionizing the banking industry by allowing banks to upgrade their IT infrastructure, stimulate innovation, and provide improved customer experiences in an increasingly digitized and competitive world. However, successful adoption necessitates a deliberate strategy that weighs the advantages of cloud computing against the banking industry's distinct problems and requirements.

The banking business faces many of the same IT difficulties as other industries, such as the need for modernization and the demand to leverage data to establish and maintain better client experiences and relationships. Banking organizations confront some of the most demanding security challenges and compliance regulations in any industry (Achuthan, 2019).

Cloud computing is categorized into three main service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS provides virtualized computing resources such as servers, storage, and networking on a pay-as-you-go basis, allowing

businesses to scale their infrastructure as needed. PaaS offers a complete development environment with tools, frameworks, and infrastructure to build, test, and deploy applications without the complexity of managing hardware. SaaS delivers fully developed software applications over the internet, eliminating the need for installation or maintenance.

Cloud deployment models define how cloud services are managed and accessed, with different approaches catering to various business needs. Public clouds are owned and operated by third-party providers, offering scalable resources to multiple users over the internet. Private clouds, on the other hand, are dedicated to a single organization, providing enhanced security and control. Hybrid clouds combine public and private cloud environments, allowing data and applications to be shared across them for greater flexibility. Community clouds serve specific groups or industries with shared infrastructure, such as government agencies or financial institutions with common regulatory requirements. Lastly, Multicloud strategies involve using multiple cloud providers to optimize performance, reduce vendor dependency, and enhance resilience. Each of these deployment models provides organizations with varying levels of control, security, and scalability based on their specific operational and regulatory needs.

1.2 Statement of the Problem

The primary focus of this paper revolves around addressing the challenges faced by banks, aiming to alleviate their burden concerning IT infrastructure management and associated costs. Instead of diverting resources towards IT infrastructure, banks should concentrate on their core financial operations. However, this necessitates a dedicated entity within the bank to oversee and manage the IT sector effectively. This is where cloud computing steps in, offering a solution that delegates the task management responsibilities to organizations in need of such services.

Studies has been done by (Begna, 2017) regarding Cloud Computing Readiness Assessment For Banking Sector In Ethiopia but the study doesn’t include local cloud service providers.

The adoption of cloud computing brings with it a myriad of advantages and disadvantages. For banks, managing security, data governance, and ensuring data availability can be particularly daunting, especially considering the sensitive nature of financial data. The apprehension surrounding storing financial data in an unknown location further complicates matters. To address these concerns, local cloud service providers in Ethiopia have begun taking proactive measures.

This local approach holds promise for Ethiopian banks, offering a more tailored and localized solution to their cloud computing needs.

Exploring Factors That Affect The Decision To Adopt Cloud Computing Technology In Ethiopian Banking Sector has been studied by (Bekele, 2014) and studied some banks and NBE to assess the readiness to migrate to cloud. Both (Begna, 2017) and (Bekele, 2014) considered international cloud while doing their studies which in Ethiopian context is not allowed to store financial data outside the country's borders.

In order to delve deeper into this issue, this paper aims to investigate the benefits, challenges, and limitations associated with local cloud service providers offering their services to banks in Ethiopia. Specifically, the study examines how local cloud service providers can enhance the banking sector's efficiency and security compared to relying solely on international cloud services. By exploring these aspects, the paper seeks to provide insights into the feasibility and efficacy of leveraging local cloud services to address the unique challenges faced by banks in Ethiopia when it comes to cloud storage and IT management.

Cloud technology links together a network of virtualized computers that are dynamically deployed as computing resources, guided by agreements between service providers and users. It offers a variety of information technology resources in different service formats, and the proliferation of cloud services on the internet brings forth new challenges in discovering and selecting suitable cloud services. To tackle these challenges, numerous studies have been conducted to develop improved methodologies aimed at aiding service consumers in selecting appropriate services. This study specifically focuses on the challenges faced by local cloud service providers and banks in Ethiopia.

A Cloud Computing Framework for Ethiopian Banking Industry has been developed by (Abere, 2014) , by considering the rule that financial data stays within the country's borders he came up with a framework for banks in Ethiopia to have a hybrid cloud of their own infrastructure and a shared cloud environment with other banks, which still doesn't divert the banking sector's concern from building IT infrastructure.

The banking sector encounters several obstacles when embracing cloud computing, and likewise, cloud service providers encounter challenges when catering to the banking sector. This research

intends to investigate how these challenges can be mitigated when cloud services are offered by local providers and what additional challenges banks might confront when utilizing cloud services from local providers.

The banking sector prioritizes the enhancement of security and reliability in its services, alongside efforts to increase service availability and reduce costs. To achieve these objectives, banks must implement comprehensive security measures, compliance protocols, data protection mechanisms, and integration strategies. These factors are often identified as the primary barriers to the banking sector's migration to the cloud.

Their studies have shown that the main concern regarding cloud adoption is security, as Ethiopia's sole national Information and Network Security protector INSA should have been included in the studies to make the security requirements clear and study the security concerns of the banks.

Studies done so far doesn't still provide a solution for the bank's investment on huge IT infrastructures needed for the operation and it doesn't shift the bank's focus off IT Infrastructure.

To deal with this, this research incorporated INSA for Security requirement, NBE for rules that govern Banks in Ethiopia and cloud service providers in Ethiopia and tried to identify what the challenges are when it comes to moving banks in Ethiopia to cloud services provided by cloud service providers in Ethiopia.

1.3 Research questions

What are the challenges of banks when it comes to moving to cloud services provided by local cloud service providers instead of building huge Data Centers?

What are the challenges of the local cloud service providers when it comes to providing their services to Banks in Ethiopia?

1.4 Objective of the Research

1.4.1 General Objective

The objective of this research is to eliminate the banks focus from IT and to let their IT needs provided by cloud computing service provider specifically local cloud service providers by identifying the challenges and benefits for banks in Ethiopia when moving to local cloud services and identifying the challenges faced by local cloud service providers in serving banks in Ethiopia. IT is considered the backbone of the Banking Industry and because of that banks invest

unbelievable amount of resource in building huge IT infrastructures instead of focusing on the business due to different reasons.

1.4.2 Specific Objective

The specific objective of this research is to enable banks in Ethiopia use cloud computing service provided by local cloud service providers.

1.5 Study motivation

Cloud technology connects a network of virtualized computers that are dynamically deployed as computing resources based on service provider and user agreements. It provides information technology resources in a variety of service formats, and the expansion of Cloud services on the Internet introduces new issues in Cloud service discovery and selection. To address these issues, a number of studies have been conducted in order to develop enhanced methodologies that will assist service consumers in selecting appropriate services.

Local cloud service providers are here providing their services for different companies with a little compute infrastructure need as compared to banks and banks are not using the service as expected or they are only using local cloud services mostly for minor services because of different challenges of cloud computing like security, availability and governance law. This study plans to narrow the gap between local cloud service providers and Banking Sector in Ethiopia by identifying benefits and challenges of local cloud service providers for the Banking sector in Ethiopia and challenges of banks in Ethiopia to use services provided by local cloud service providers.

Since Cloud computing has the potential to significantly impact banking operations, including cost reduction, scalability, agility, and improved customer experiences and banks face a lot of challenges to migrate to cloud the benefits and challenges should be studied to provide a way for the Bank’s to use cloud computing.

I believe that the banking sector should adopt cloud computing technologies to improve operational efficiency, enhance customer experiences, and drive innovation. The banking industry is undergoing significant digital transformation, and cloud computing plays a critical role in this process. Researching local cloud computing service provider’s for the banking sector can not only help the local cloud service providers to know and fill the gap but can also contribute to banks'

transformation efforts, assisting them in leveraging the benefits of local cloud technology or service while addressing their unique challenges and requirements.

1.6 Significance of the study

Cloud computing has a tremendous impact on information technology and is a key technological driver of enterprise digitalization. However, as cloud services become more widely available and the number of cloud service providers grows, so does the uncertainty and risk for user firms in embracing cloud services.

The environment of cloud computing is continually changing, with new technology and market trends emerging. Understanding the issues that cloud service providers face helps in keeping up with these developments, adjusting to new technology paradigms, and meeting changing consumer demands.

Cloud service providers may improve their service offerings, boost customer satisfaction, and stimulate innovation in the cloud computing sector by researching and addressing these difficulties. The cloud computing sector has made a wide range of service options available to customers. In today's computing environment, the number of cloud service providers and their offerings is growing at an exponential rate. In such a case, the customer must choose the best cloud service provider based on his specific quality of service requirements.

Whatever the case banks need to minimize their cost on IT infrastructure and avoid building huge data centers with expensive IT infrastructure and avoid the cost of employing IT literate staffs and paying for expensive trainings.

This research helps banks and local cloud service providers see what the challenge is for both and what standards are there and what other standards are missing for the provider to provide their services and for the customer to use the services.

1.7 Scope of the study

The adoption of cloud service for the banking industry has its own benefits and challenges but, even thou cloud service providers and Banks face challenges everywhere, the scope of this study is limited to cloud service providers in Ethiopia and Banking sector in Ethiopia.

CHAPTER TWO

LITERATURE REVIEW

2.1 INTRODUCTION

Banks represent a crucial sector that cloud computing is increasingly focusing on in the foreseeable future. Given the unique demands of banking operations, cloud services must offer solutions akin to a "silver bullet." Cloud computing presents numerous advantages for banks as customers. Foremost among these advantages is cost-effectiveness, as leveraging cloud servers instead of maintaining personal servers can lead to substantial savings. Additionally, cloud services offer several other benefits like Usage-Based Billing, Business Continuity, Business Agility, and Green IT. (Nedelcu & Stefanet, 2019).

Cloud computing presents a compelling proposition for banks seeking to modernize their IT infrastructure, improve operational efficiency, and stay ahead in a rapidly evolving digital landscape. By embracing cloud services, banks can unlock new levels of agility, resilience, and cost-effectiveness while driving sustainable growth and delivering superior value to their customers.

Cloud computing represents a game-changing paradigm in the banking industry, allowing institutions to acquire and use IT resources in previously unheard-of ways. The ability to successfully use this technology will be critical in establishing a competitive advantage and providing outstanding service to clients. This impetus comes at a time when banks are under increasing pressure to streamline their IT expenditures while maintaining a high level of service delivery. One of the primary benefits of cloud computing is the potential to provide high levels of redundancy and backup capabilities at a cheaper cost than traditional managed solutions. This redundancy promotes continuity of operations and decreases the danger of data loss or service disruptions, strengthening the resilience of banking systems in the face of unforeseen occurrences or cyber threats (Hailu, 2020).

2.2 Types of cloud Computing

• **Infrastructure as a Service (IaaS):** This service provides users with the core components of cloud computing, including servers, storage, and networks. Users can utilize these resources to run their own programs and operating systems, which gives them more control.

Infrastructure as a Service is a type of hosting. It covers network access, routing, and storage. In general, the IaaS provider will supply the hardware and administrative services required to host applications, as well as a platform for operating them. Scaling of bandwidth, memory, and storage is typically included, and vendors compete based on the performance and cost of their dynamic services. The service provider owns the equipment and is responsible for housing, operating, and repairing it (Bhardwaj et al., 2010).

• **Platform as a Service (PaaS):** This service offers users a pre-built environment in which to develop, test, and deploy cloud apps without worrying about the underlying infrastructure. Users may create more flexible apps by combining a range of tools and frameworks.

PaaS is a type of cloud computing approach in which a platform serves as an environment for application development. Where developers can use the essential libraries, programming languages, services, and other GUI-based tools from the cloud (Laghari et al., 2018).

• **Software as a Service (SaaS):** This service provides consumers with ready-to-use cloud-based apps that they do not need to install or administer themselves.

The Software as a Service (SaaS) model provides the advantage of renting software from a cloud computing vendor at a low cost rather than purchasing and managing it at a high cost. Vendors may provide SaaS as a managed service on a leasing basis, making it affordable and lowering maintenance costs (Levinson, 2007). SaaS decreases an organization's software acquisition risk, allowing it to fulfill business goals more quickly.

2.3 Cloud Deployment Models

The different cloud deployment models listed here are models derived from a comparative study of cloud deployment models by (B. Patel & Kansara, 2021).

1. Public Cloud: The public cloud is a type of cloud computing model in which cloud services and infrastructure are provided by third-party cloud service providers over the internet. In a public cloud environment, multiple users and organizations share the same pool of computing resources, including servers, storage, networking, and applications, which are hosted in data centers operated and managed by the cloud provider. The public cloud model represents a widely embraced form of cloud service, wherein the entirety of the hardware necessary to facilitate the public cloud is owned and managed by the service provider. These hardware components are housed within

expansive data centers maintained by the vendors. The public cloud delivery approach holds significant relevance, particularly in the realm of development and testing (B. Patel & Kansara, 2021). In this context, a third-party cloud service provider assumes ownership and responsibility for maintaining the infrastructure supporting the application or service. Consequently, a multitude of clients share these resources, with the service provider taking charge of the management and upkeep of the underlying infrastructure.

2. Private Cloud: A private cloud refers to a cloud computing environment dedicated exclusively to a single organization, whether that organization is a business, government agency, or other entity. Unlike public clouds, which serve multiple users and organizations, private clouds are designed to meet the specific needs and requirements of a single entity.

A private cloud belongs to a certain organization. That organization oversees and operates the system centrally. Private cloud servers can be hosted by a third party (such as a service provider). Most businesses choose to maintain their gear in a local data center. From there, an internal team may monitor and manage everything (B. Patel & Kansara, 2021). In a private cloud deployment, the cloud infrastructure, including servers, storage, networking, and software applications, is either hosted on-premises within the organization's data center or hosted by a third-party provider on a dedicated infrastructure. This infrastructure is typically managed and maintained solely for the use of the organization and is not shared with other users or organizations.

A private cloud is characterized by dedicated resources, security and compliance, isolation, customization and control.

3. Hybrid Cloud: A hybrid cloud is a cloud computing platform that contains components of both public and private clouds, allowing businesses to reap the benefits of both models. In a hybrid cloud deployment, some workloads and data are kept and managed in a private cloud, while others are hosted in a public cloud architecture. The two environments are frequently linked, allowing for smooth data and application portability and easing communication between public and private cloud components. Hybrid clouds represent a fusion of public and private cloud environments, strategically designed to facilitate seamless data and application integration while promoting effective communication between the two platforms (B. Patel & Kansara, 2021). This hybrid cloud deployment model integrates elements from both public and private clouds, offering enterprises a versatile approach to managing their workloads.

By leveraging hybrid cloud solutions, organizations can harness the scalability and cost-efficiency of public clouds for certain workloads, optimizing resource utilization and minimizing operational expenses. Meanwhile, sensitive data and critical applications can be safeguarded within a private cloud environment, where enhanced protection measures and stringent controls ensure confidentiality and compliance with regulatory standards.

The flexibility inherent in hybrid cloud deployments empowers enterprises to strike a balance between scalability and security, tailoring their infrastructure to meet the unique requirements of each workload. Through seamless integration between public and private clouds, organizations can achieve a cohesive and agile IT environment capable of supporting diverse business needs and driving innovation.

4. Community Cloud: A community cloud service is a cloud-based platform that caters to a group of users or organizations with common interests or objectives. These organizations typically share similar missions, governance structures, security requirements, and policies. The deployment of a community cloud service can vary, with options including hosting on the premises of the consumer organization, the premises of peer organizations, or a combination of both (B. Patel & Kansara, 2021). The community cloud deployment model revolves around the concept of sharing cloud infrastructure among multiple entities with comparable interests or needs. This arrangement facilitates collaboration and resource sharing among enterprises while still maintaining isolation and control over individual data and operations. In essence, community cloud empowers organizations to leverage shared resources and capabilities while retaining autonomy and governance tailored to their specific requirements.

By embracing community cloud deployment, organizations can unlock various benefits, including enhanced collaboration, cost efficiency through resource sharing, and streamlined management of shared infrastructure. Additionally, the community cloud model offers a flexible and scalable solution that adapts to the evolving needs and priorities of participating organizations.

5. Multi-Cloud: Multi-cloud refers to the utilization of two or more cloud computing services sourced from various providers in the cloud ecosystem. Such an environment can encompass either entirely private, completely public, or a hybrid blend of both infrastructures. Businesses opt for a multi-cloud approach to efficiently allocate computing resources and mitigate risks associated with potential downtime and data loss (B. Patel & Kansara, 2021). This strategy involves leveraging

diverse cloud service providers to host distinct components of an application or service, offering advantages such as flexibility, redundancy, and access to specialized services from multiple sources.

Selection of a deployment model is guided by various criteria, including security requirements, scalability needs, cost considerations, and organizational preferences. Whether opting for a private or public cloud model, the overarching objective of cloud computing remains consistent: to provide accessible, scalable access to IT resources and services. Cloud service providers typically offer resources on a pay-per-use basis, enabling users to scale resources up or down according to their specific requirements. This pay-as-you-go model encourages businesses to migrate their applications to cloud infrastructures, thereby avoiding significant upfront investment costs.

However, the abundance of cloud service providers and functionally equivalent services available in the market presents challenges for customers in selecting the most suitable and efficient provider. Despite assurances provided in Service Level Agreements regarding quality parameters, cloud service providers often encounter difficulties in fulfilling these promises due to various challenges they face. As such, navigating the landscape of cloud service providers requires careful consideration and evaluation to ensure optimal selection and service delivery alignment with organizational needs.

2.4 Cloud Computing for Banks

The financial sector faces a distinctive challenge, balancing the opportunity to extend banking services to millions of unbanked individuals while contending with disruption from cloud-native fintech enterprises. This dichotomy underscores the critical need for the financial industry to embrace digital transformation to secure its relevance and competitiveness in a rapidly evolving landscape. Financial sector needs to manage & extract data, often in collaboration with cloud-native start-ups, while ensuring their long term operational resilience. Cloud adoption supports these goals, making it necessary to the operations of any modern digital businesses, and bringing benefits not only to incumbents but also to newcomers, customers & economy as a whole. It provides infrastructure and advanced analytics in the speed required by digital transformation, and to a level that financial sector cannot match with their own in-house IT support (Hajizadeh & Hajizadeh, 2020).

Cloud computing represents a groundbreaking technology that has revolutionized the storage, processing, and analysis of data within the banking sector. Through harnessing the capabilities of the cloud, financial institutions can avail themselves of a diverse array of IT services and software applications to streamline operations and foster innovation. Cloud computing eliminates the necessity for banks to uphold extensive on premise data centers or make substantial investments in hardware and software infrastructure. Instead, they can adopt a pay-as-you-go model, accessing computing resources as needed and adjusting their usage levels accordingly. This flexibility enables banks to exhibit greater agility and responsiveness to evolving business requirements, all while circumventing the upfront expenses and maintenance burdens associated with traditional IT setups (Smusin, 2023).

2.5 Challenges of cloud Computing

In today's world, cloud computing services have some limitations that discourage banks from adopting them. These problems typically revolve around concerns of security, data confidentiality, and the reliability of service delivery. Navigating these problems needs a determined effort by banks to handle the bits of cloud computing adoption while limiting associated risks. Banks can overcome these challenges by implementing comprehensive risk management strategies, adopting best practices in data security and compliance, and cultivating strategic partnerships with reputable cloud service providers.

Ensuring the utmost confidentiality and security of both financial and personal data, along with mission-critical applications, stands as an imperative priority. Banks cannot overlook the potential risks posed by security breaches. Preserving the confidentiality and security of both commercial and personal data, alongside mission-critical applications, holds paramount importance. The financial services industry presents unique challenges in maintaining the security of financial data, encompassing concerns such as data leakage, unauthorized usage, loss, and authentication. Ultimately, for cloud computing to garner complete acceptance within the banking services sector, it necessitates seamless integration of cloud services into existing security frameworks and procedures (Bejju, n.d.).

The assertion is made that a parallel can be drawn between the progression of Internet Banking and cloud computing due to their apparent shared challenges concerning security.

Security issues were likewise a hindrance during the initial stages of internet banking adoption, which could be seen as a precursor to cloud computing. Similarly, if cloud computing enterprises persist in addressing market apprehensions regarding the safety, cost-effectiveness, and convenience of cloud computing, it is anticipated to achieve the ubiquity observed in online banking and other internet-based financial activities today (Nedelcu & Stefanet, 2019).

1. **Security and Data Protection:** Banks handle highly sensitive consumer information, especially financial data, making security and data protection paramount. When transitioning data and applications to the cloud, ensuring security and data protection becomes a primary concern. To safeguard against data breaches and unauthorized access, banks need to ensure that their chosen cloud service providers implement robust security measures. These measures may include encryption, access controls, and intrusion detection systems to mitigate risks effectively.

   Based on the International Data Corporation (IDC) survey, the foremost concerns in cloud adoption are Security, Performance, and Availability. The primary challenge lies in effectively managing security and privacy issues arising from data and application migration across networks. This includes addressing concerns related to data control, the diverse array of resources, and the differing security policies enforced within cloud environments (Sajid & Raza, 2013).
2. **Regulatory Compliance:** As cloud computing adoption grows, banks are expected to own and manage the cloud infrastructure, while service providers take on more responsibility. A clear strategic policy for cloud computing and administration is necessary, prioritizing data that can be trusted to the cloud operator. Service level agreements (SLAs) should be developed with milestones and timeframes, supported by a robust governance framework (Achuthan, 2019).Banks need to ensure that their chosen cloud service providers adhere to industry standards and regulations, equipping them with the necessary tools and functionalities to fulfill their compliance responsibilities. This involves thorough vetting of cloud providers' adherence to established standards, coupled with robust mechanisms to verify ongoing compliance. Additionally, banks should seek providers who offer comprehensive compliance features tailored to the banking sector's unique regulatory landscape, ensuring seamless integration of compliance measures within their cloud-based infrastructure.

3. **Data Sovereignty and Residency:** Customers bear significant responsibility for ensuring the safety and reliability of their information, even when entrusted to service providers. Traditional services prioritize external audits and safety certifications. Banking regulators often require financial data for customers to remain within their home country, and compliance regulations mandate the separation of certain information from shared servers or databases. It's crucial for banks to precisely know the location of their data in the cloud (Achuthan, 2019). Banks frequently face legal and regulatory obligations regarding the location of consumer data storage and processing. They may need to ensure that data stays within particular geographic bounds or is directly under their control. To achieve these standards, cloud service providers must provide options for data residence and sovereignty.
4. **Service Availability and Reliability:** Downtime and service outages, often caused by internet connectivity issues, can have a significant impact on banking operations. Even a brief network or internet disruption lasting a few minutes can lead to substantial consequences, such as failed transactions or loss of critical data exchanges. Over the course of a year, these interruptions can accumulate, potentially resulting in considerable operational inefficiencies and financial losses for the bank (Nedelcu & Stefanet, 2019).

   Banks operate continuously, and any interruptions or delays in service can lead to significant financial losses and damage to their reputation. It is imperative for banks to verify that their cloud service providers guarantee high availability, robust disaster recovery protocols, and enforce service level agreements (SLAs) to maintain consistent uptime and performance.
5. **Cyber Crimes:** In our increasingly technologically advanced world, it's widely acknowledged that cybercrime is also advancing. This encompasses activities like hacking and uploading viruses, among others. These cyber threats present significant risks across all sectors. Despite the availability of various detection and prevention methods, completely eradicating cybercrime is nearly impossible. Consequently, bankers exhibit considerable reluctance to transition from traditional service providers to cloud computing service providers. The fear stems from the potential loss of data or funds due to breaches in the bank's server or cloud server, which could impose a substantial burden on the bank if such incidents occur (Dennis & Ravi, 2019).
6. **Legacy Systems and Integration:** Banks frequently deal with complicated IT environments characterized by legacy systems and a wide range of applications. Integrating these systems

with cloud-based apps is difficult due to compatibility difficulties. As a result, banks must ensure that the cloud service providers they choose enable seamless integration and interoperability with current systems.

Because integration depends on the availability and dependability of the internet connection and network bandwidth, as well as the cloud platform, security and compliance needs of the data and applications, and the cloud architecture, the integration of cloud with the existing system is easier for local cloud service providers

7. **Flexibility:** Banking professionals who adopt cloud computing encounter constraints in flexibility. This arises from their reliance on cloud-based systems for data storage, limiting their ability to make critical decisions autonomously. Consequently, this diminishes their flexibility in decision-making processes and other areas.
   Indeed, this represents a significant concern contributing to the reluctance of banking sectors to embrace cloud computing. Furthermore, optimal flexibility is essential for banks to execute their operations with enhanced efficiency and effectiveness. (Dennis & Ravi, 2019).
8. **Vendor Lock-In:** When using cloud computing, banks must consider the risk of vendor lock-in. They should have mitigating measures in place, such as cloud-agnostic architectures or multi-cloud approaches, to maintain flexibility and avoid reliance on a single cloud service provider.

   While cloud computing has many advantages, there are also obstacles and considerations that enterprises must face. Vendor lock-in is a potential danger since enterprises may become significantly dependent on a specific cloud provider's proprietary technologies and struggle to shift to other platforms. (Joe, 2023).
9. **Misunderstanding of responsibilities:** In a typical context, the security of data is entirely the responsibility of the company that owns data. In a cloud computing context, two actors share responsibilities: the cloud provider and the customer. There is a great possibility for erroneous risk management decisions if cloud providers do not disclose the extent to which the security measures are implemented and the consumer knows which controls are still needed to be adopted. (Hajizadeh & Hajizadeh, 2020). So misunderstanding of responsibility can also lead to security risks because the cloud providers will assume the banks will protect access to their data and banks will assume the cloud service providers will block unnecessary access to the banks financial data. Which means there might me a clear communication barrier

regarding data security layer or to what extent the cloud service provider is expected to implement security.

10. **Data Recovery:** In the event of data loss, it's critical for complete data recovery to be ensured, prompting inquiry into whether cloud service providers possess the capability to fully restore lost data. This concern regarding data restoration proficiency serves as a potential deterrent for banks considering the adoption of cloud computing. (Dennis & Ravi, 2019).

2.6 Why Local Cloud

Cloud computing does more than merely facilitate collaborative tasks. Furthermore, it reduces the need for businesses to invest in fancy computers, data servers, pricey software that is only used once a month, maintenance and support personnel, and a variety of other expenses. What you need is a relatively simple computer connected to the Internet, some basic software, such as a free browser, and a pay-as-you-go subscription to the services that you require (de Bruin & Floridi, 2017). If certain obstacles, such as Security and Data Protection, Regulatory Compliance, Data Sovereignty and Residency, Service Availability and Reliability, and Cost Management, can be alleviated or surpassed by utilizing local cloud service providers, it raises the question: why not use them? While global cloud giants offer extensive resources and capabilities, local cloud service providers often offer distinct advantages that cater to specific needs and concerns of businesses, particularly those in regulated industries like banking.

By leveraging local cloud service providers, banks can potentially address key challenges more effectively. These providers may offer:

Enhanced Regulatory Compliance: Local cloud service providers are generally well-versed in local rules and compliance requirements, allowing banks to smoothly satisfy regulatory standards and overcome legal complications. Different national and organizational rules will be simple to apply because they are enforced on enterprises inside the same country. Rules like data protection, when overseas cloud service providers fail to comply, and various other rules. Banks fail to comply while using cloud services offered by overseas service providers. Because of the importance of financial information, local laws require financial institutions such as banks to know exactly where their customers' data is maintained.

Many banking regulators demand that functional data for banking customers remain within their own nation. Certain compliance regulators require that data not be combined with other data in shared servers and databases. This suggests that banks should keep in mind where their data is stored in the cloud. This is one of the key issues in cloud banking, since bankers find it nearly impossible to determine exactly where their data resides on the cloud. This is because all data in the cloud coexists with each other. As a result, this could represent a significant threat to the banking sector (Dennis & Ravi, 2019).

Data Sovereignty and Residency: Local suppliers may provide assurances on data sovereignty and residency, guaranteeing that sensitive data is kept within the country's boundaries and adheres to local data protection rules. One of the benefits of using a local cloud service is that the data is closer to the bank's location and it is easier to know where exactly customer data is stored. This is because local cloud service providers have their data centers in the same country as the bank (Cloud251, 2024).

Improved Service Availability and Reliability: Local providers may provide specialized support and services aimed at increasing service availability and dependability, reducing downtime and maintaining smooth operations for crucial banking functions. Data and applications are stored and processed at places near their origin and destination.

Free cloud services and products can be easily developed and deployed, offering banks a seamless way to enhance their capabilities. With cloud solutions, banks can scale their computing power to handle peak demand efficiently without needing to invest in or upgrade their existing technology infrastructure. This scalability ensures smooth operations during high-demand periods while minimizing costs and resource constraints (Nedelcu & Stefanet, 2019).

Local cloud reduces latency and improves performance by storing and processing data close to the users and apps that use it, rather than relying on an internet connection to receive data from remote servers. This reduces network latency and bandwidth consumption, both of which can affect the performance and quality of cloud services. In the event of an internet disruption or outage, a local cloud can be used as a backup or fallback solution.

Cost Reduction

By transitioning to cloud services, banks can avoid the significant costs associated with purchasing dedicated hardware, premium software, and hiring highly skilled professionals. This shift can result in substantial financial savings, as cloud providers typically handle updates and maintenance of the IT infrastructure at no additional cost. Moreover, the pay-as-you-go model allows banks to pay only for the resources and technology they actively use, ensuring cost efficiency by aligning expenses with actual operational needs. This flexible approach not only reduces upfront investments but also eliminates the ongoing burden of managing and upgrading complex IT systems, enabling banks to focus on their core financial operations (Achuthan, 2019).

Additionally the cost reduction will be like hitting two birds with one stone because it is beneficial for Ethiopian banks when the cloud service is provided by local cloud service providers because it also saves the huge amount of local currency so that they get services with Ethiopian Currency (Cloud251, 2024).

Greater customization and flexibility

The flexibility offered by a cloud platform enables businesses to adapt swiftly to changing market conditions, evolving customer demands, and advancements in technology. This agility ensures that organizations can scale resources up or down as needed, maintain operational efficiency, and deliver enhanced customer experiences. The ability to quickly adjust capacity becomes a significant competitive advantage, empowering businesses to stay ahead in dynamic markets and seize opportunities with minimal delay (Nedelcu & Stefanet, 2019).

When it comes to local cloud service providers, customization and flexibility concerns are reduced. Local providers can give personalized support and customized solutions geared to the individual needs of banks, resulting in a higher level of responsiveness and flexibility than bigger global providers. Furthermore, collaborating with local cloud providers can help to expand and strengthen the local economy by encouraging innovation, creating job opportunities, and promoting the country's digital ecosystem.

The decision to use local cloud service providers is based on a variety of variables, including the bank's specific objectives and priorities, regulatory requirements, risk tolerance, and the availability of suitable providers in the local market. While global cloud giants provide vast resources and capabilities, local providers may provide specialized expertise and services that are

more closely aligned with the specific needs and challenges that banks encounter in their operational environment.

Private and business consumers are increasingly turning to the cloud as their preferred solution. The advantages are enormous: no installation, configuring, updating, or upgrading, no compatibility difficulties, low prices, and computing power that much exceeds that of their own PCs, servers, and datacenters. This is especially enticing to many commercial firms who have seen a data explosion (known as Big Data) that their in-house computing capabilities can no longer handle (de Bruin & Floridi, 2017).

2.7 Theoretical Frameworks

Adoption of new technologies is complex and requires a careful study. Researchers have developed many adoption models. Among these are the Technology Acceptance Model (TAM), Unified Theory of Acceptance and Use of Technology (UTAUT), Diffusion of Innovation (DOI), and the Technology-Organization-Environment (TOE) framework.

1. The Technology Acceptance Model (TAM)

Is an information systems theory that describes how to persuade consumers to accept and use new technology (Davis, 1989). It has been widely employed by information systems scholars to address the difficulty of organizations in fostering acceptance of new information systems (Venkatesh & Davis, 2000).

Fred Davis invented TAM in 1986, and it is founded on the premise that two fundamental aspects impact human attitudes toward technology: perceived utility and perceived ease of use. Perceived usefulness is the extent to which we believe that utilizing technology will improve our performance or help us achieve our goals, whereas perceived ease of use is the degree to which we believe that using technology will be simple and easy (Venkatesh & Davis, 2000).

According to TAM, these two elements are the key predictors of our intention to utilize a technology, which then predicts our actual usage behavior. In other words, if we believe a technology is valuable and simple to use, we are more inclined to adopt and implement it.

2. The UTAUT framework

The UTAUT framework integrates numerous adoption theories and models, including TAM and the Theory of Reasoned Action, to study information technology adoption in organizations. The

UTAUT combines existing and tested theoretical frameworks to provide a unified perspective on user acceptance of new technologies.

The UTAUT model expanded on the TAM theory by incorporating two additional variables: social influence and facilitating conditions. The key factors from the TAM model, perceived ease of use and perceived usefulness, which are considered crucial for predicting behavioral intention to adopt new technology, are retained in the UTAUT model but are renamed as Performance Expectancy and Effort Expectancy, respectively. Additionally, four moderators were introduced in the UTAUT model to explore their moderating effects on users' intention and behavior in the context of technology acceptance and usage(Riad Jaradat et al., 2020).

According to UTAUT, performance expectancy, effort expectancy, and social influence all influence behavioral intentions toward technology use, which predicts actual system use.

Performance Expectancy (PE) refers to how using a technology will benefit users during their activities.

Effort Expectancy (EE) refers to the ease with which technologies are used.

Social Influence (SI) refers to the degree to which individuals perceive the society (family, friends) believe they should use the technology.

Facilitating conditions (FC) refers to the individual's beliefs of the availability of resources and assistance required to complete a behavior. Performance expectancy, effort expectancy, and social influence are thought to influence behavioral intention to use technology, whereas behavioral intention and facilitating conditions decide technology use (Bekele, 2014).

3. Diffusion of Innovation (DOI)

Is primarily based on technological aspects and user perceptions of innovation. Individuals are less complex than organizations.

According to (Everett M. Rogers, Arvind Singhal, 2008), creativity involves communication through multiple social channels. Three elements influence the acceptance of innovation inside businesses. Organizational characteristics include leadership attitude toward change, internal structure (centralization, complexity, interconnectivity, personnel numbers, and slack), and external system openness. There are different definitions of innovation. Innovation encompasses

new ideas, processes, products, and technologies. According to (Everett M. Rogers, Arvind Singhal, 2008) each innovation has unique characteristics that impact its adoption in society.

Each innovation's important features are relative advantage, compatibility, complexity, try ability, and observe ability. Relative advantage refers to the perceived superiority of an innovation over its predecessor. Compatibility with an innovation significantly impacts its speed of acceptance in society. Innovations that align with individual and societal norms tend to be adopted faster than those that do not. The term complexity describes "the degree to which an innovation is perceived as relatively difficult to understand and use". Usually, complexity has a detrimental impact on diffusion. Complex innovations have a lower possibility of successful diffusion throughout society. Trial ability refers to the ability to experiment with innovations on a modest scale. Finally, observe ability refers to how visible the benefits of an innovation are to others.(Amini & Javid, 2023)

4. The TOE (Technology-Organization-Environment) framework

Developed by Tornatzky and Fleischer in 1990, represents the Technology, Organization, and External Environment. These three aspects collectively impact technology adoption. By utilizing this model, leaders and managers can gain a deeper understanding of the critical factors involved, enabling them to make informed decisions and implement future improvements (Erturk, 2021).

To examine the challenges and benefits of local cloud service providers and the banking sector in Ethiopia while adopting cloud computing, this research uses Technology-Organization-Environment (TOE) framework to investigate the factors that influence cloud computing adoption. The TOE framework examines how the firm's setting affects the adoption and implementation of innovations. The TOE framework outlines how three aspects of an organization's setting influence adoption decisions. The three factors are: technology context, organizational context, and environmental context. All three are expected to impact technological innovation (Dwivedi et al., 2012).

The External Environment encompasses factors such as the business sector, market structure, and regulatory landscape. The Organization is evaluated based on its structure, size, and internal communication processes. Technology refers to a particular system or solution, including its features, availability, and practicality (Erturk, 2021).

For banks I have used the TOE framework to study how technological factors like local cloud security,, organizational factors like IT capabilities, cost management and environmental factors like regulatory compliance impact their cloud adoption decisions.
For Cloud Service Providers I have used the TOE framework to understand how they address the technological needs of banks, align their organizational resources, and respond to environmental pressures like regulatory requirements.

The key aspect of a conceptual framework is that it represents a conceptual or theoretical model of the subject you intend to study. It outlines what exists in the area of investigation, what processes are occurring, and why these phenomena might be taking place. Essentially, it serves as a preliminary theory of the topic being explored. This framework plays a critical role in shaping the overall research design. It guides you in refining your research objectives, formulating clear and relevant research questions, selecting suitable methods for data collection and analysis, and identifying potential validity threats that could compromise your conclusions. Additionally, the conceptual framework strengthens the rationale for your study by providing a structured basis to explain the importance and relevance of your research (Maxwell, 1941).

In summary, the TOE framework is well-suited to studying the complex interplay of factors affecting local cloud service adoption in the banking sector, providing a holistic view of the challenges and benefits for both banks and cloud service providers.

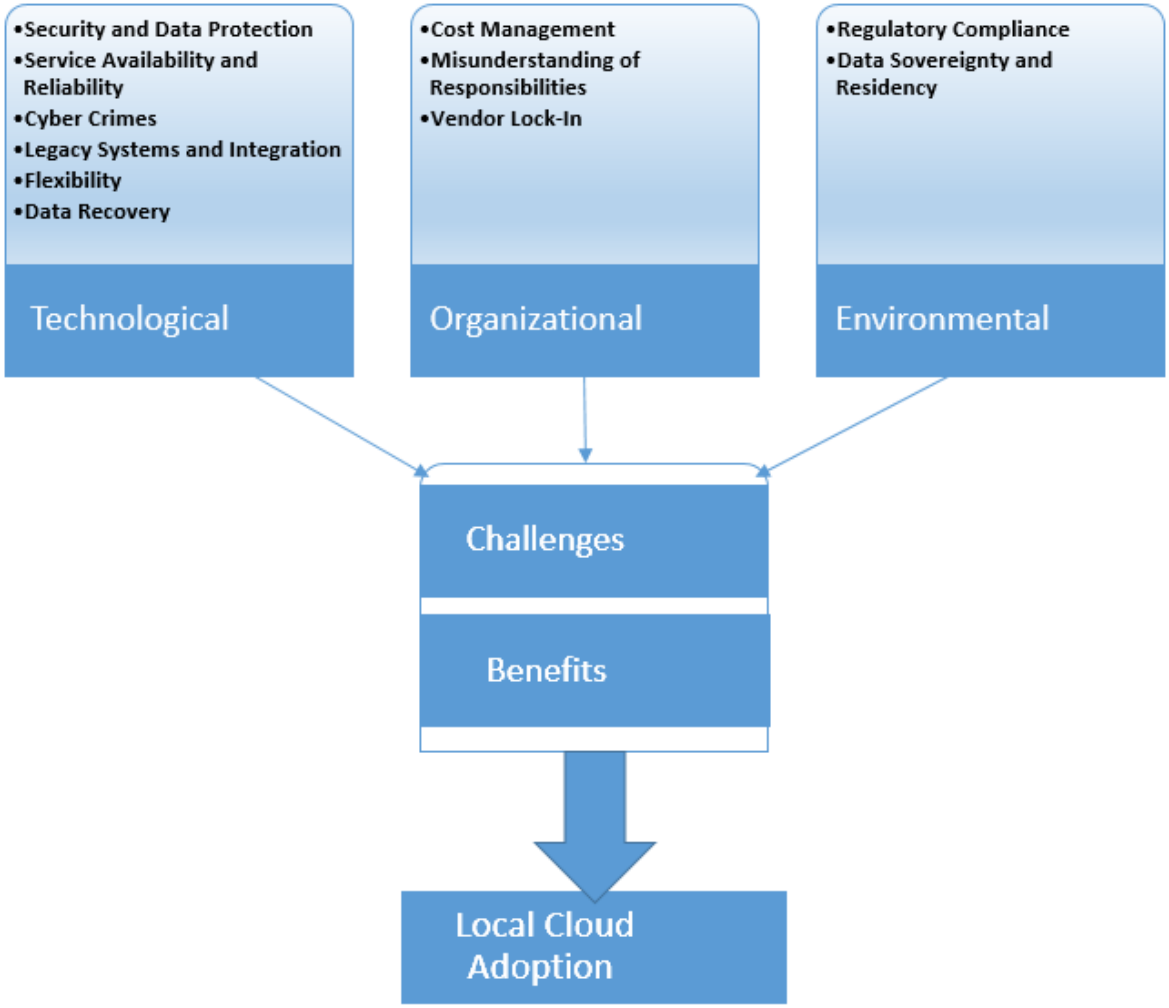

Figure 1: Adopted and Modified Framework for the study

2.8 Cloud Service providers in Ethiopia

Currently there are many cloud computing service providers in Ethiopia and some of the providers with the ability and willingness to provide cloud services to banks in Ethiopia are listed below with the services they provide to the banking sector in Ethiopia.

1. Telecloud by Ethio Telecom

Ethio Telecom, the largest telecom operator in Ethiopia, launched Telecloud as part of its diversification strategy to provide cloud-based solutions. It aims to meet the growing demand for digital infrastructure and cloud services across the country. Telecloud's infrastructure is based in Ethio Telecom's data centers, ensuring high levels of availability and uptime. This collaboration is designed to increase efficiency for local businesses by providing access to high-quality cloud

services without relying on international providers. Telecloud claims to provide Innovative, Trustworthy, and Secure Products and Services and they Work together with high-quality partners to build cloud ecology and boost industrial development while providing full- stack solutions for any industry (Ethio telecom, 2024).

Services Provided: according to (Ethio telecom, 2024)these are the services provided by Telecloud.

- **Storage Services:** TeleCloud offers different scalable and secure cloud storage options for businesses. These services help companies store, access, and manage data on-demand without relying on physical storage infrastructure.
- **Compute Services:** Virtualized compute resources are available, allowing businesses to run applications on-demand without maintaining their own hardware.
- **Network Services:** Provides redundant and robust network solutions, including VPNs and high-speed connectivity to ensure secure data transfer and business operations.
- **Security Services:** TeleCloud offers enhanced security features like firewalls, intrusion detection systems, and encryption services.
- **Backup and Disaster Recovery:** Telecloud uses different backup methods and Ensures data is backed up regularly, with disaster recovery services to guarantee business continuity in the event of system failures.
- **Types of cloud services provided:** telecloud currently provides IaaS, PaaS and SaaS offerings for enterprises that need cloud services.
- **Support Services:** Offers 24/7 support to ensure that businesses can rely on the cloud services without disruption.

2. Zergaw Cloud

ZERGAW CLOUD is one Ethiopia's largest cloud services provider. Established in 2019 by a team of experienced and dedicated ICT professionals with an in-depth knowledge of cutting-edge cloud technology and the local market's specific requirements (Zergaw, 2023).

Our services are designed and implemented to overcome three critical challenges of the local ICT industry: unaffordable quality, slow procurement and deployment, and frequent system down with

slow maintenance. Our services are affordable, easy to deploy and scale, and highly reliable and available, helping businesses operate in cost and time efficient manner (Zergaw, 2023).

Zergaw Cloud is a local cloud service provider that focuses on providing affordable and flexible cloud services tailored to the Ethiopian market. It has grown in popularity for offering a reliable, localized solution for businesses needing cloud infrastructure.

Services Provided: according to (Zergaw, 2023) these are the services provided by Zergaw Cloud.

- **Compute and Storage Services:** We offer scalable cloud servers with dedicated computing and storage resources (SSD or HDD) from our cutting-edge infrastructure, hosted in Ethiopia's most secure and reliable locations.
- **Security Services:** We ensure customer protection by adhering to the ZERGAW Cyber Security Framework (Z-CARE), which is built on NIST CSF and INSA Critical Mass. Our approach includes advanced multi-layered security technologies, a Zero-Trust Model, and a sophisticated Security Operations Center (SOC) for proactive monitoring and response. Additionally, we provide tailored security solutions like firewalls and email protection.
- **Network Services:** Offers managed networking services to ensure smooth and secure data transfer between clients and the cloud. Our cloud servers can be hosted and accessed over the Internet or VPN, while Bare Metal Servers are customizable to your specific needs and managed through a secure web-based interface. With 99.95% availability, our cloud infrastructure is located near the national backbone network for optimal stability and connectivity.
- **Backup and Disaster Recovery:** Provides data protection through regular backups and systems for rapid disaster recovery.
- **Support Services:** Offers 24/7 support to ensure that businesses can rely on the cloud services without disruption.

3. ALTA-Africom Cloud Technology Service (AACTS)

ALTA-Africom Cloud Technology Service (AACTS), established in May 2024, is a young company offering comprehensive cloud computing solutions in Ethiopia. It is a joint venture between two leading IT firms: ALTA Computec PLC, a 30-year giant in Ethiopia's ICT market, and Africom Technologies PLC, a 15-year specialist in software development and process engineering. Leveraging their combined expertise, AACTS aims to become Ethiopia's leading cloud service provider, delivering innovative and reliable infrastructure, platform, and managed cloud services to enterprises across diverse industries (AACTS, 2024).

Services Provided: according to (AACTS, 2024) these are the services provided by AACTS.

- **Data Center Services:** Provides colocation services with 24/7 monitoring to ensure the optimal performance and uptime of servers hosted within its data center.
- **Compute and Storage Services:** We offer on-demand access to scalable computing, storage, and networking resources, including virtual machines, bare-metal servers, and software-defined infrastructure. Our services ensure high availability, robust security, and compliance with industry standards.
- **Security Services:** Offers we implement robust security measures to safeguard against cyber threats while ensuring compliance with industry regulations and standards. Our services include.
- **Network Services:** We provide a comprehensive suite of networking services, including virtual private networks (VPNs), load balancing, and direct connectivity options. Our software-defined networking capabilities enable customers to create and manage their own virtual network environments seamlessly within the cloud.
- **Backup and Disaster Recovery:** Provides data backup services, ensuring that data is regularly backed up and can be restored in case of an emergency.
- **Communication (Support) Mediums:** Phone support, email support, online ticketing and self-service portal and in person support.

4. Cloud 251

Cloud 251 is Ethiopia's leading cloud service provider, delivering the reliability and features of global providers like AWS and Azure while ensuring data remains within the country and payments can be made in local currency (ETB). We aim to empower businesses and individuals with flexible, scalable cloud solutions and an intuitive user console for seamless cloud resource management (Cloud251, 2024).

Cloud 251 use a platform named Cloud 251 which is an enterprise-grade cloud storage and computing platform offering scalable, high-performance, and secure infrastructure services. It provides businesses with fully managed storage, compute, and networking solutions, deployable both on-premises and in the cloud (Cloud251, 2024).

Services Provided:

- **Compute Storage Services:** Cloud 251 provides a reliable object storage solution that allows customers to store, access, and manage their data with ease. Our service offers high durability, low latency, and scalability, ensuring your critical information is always available when needed.
- **Compute Services:** Our virtual machine service offers scalable and flexible cloud computing solutions, tailored to meet your needs. Leverage the power of virtualization to streamline workflows and enhance productivity.
- **Network Services:** Offers high-performance networking solutions, including private cloud connectivity and VPN services, for secure data transmission by using their cloud 251 solution.
- **Security Services:** they offer physical security in the data center and virtual security features like encryption and firewalls to protect cloud-based assets supported by multiple national and international security standard certifications.
- **Backup and Disaster Recovery:** cloud 251 Provides robust disaster recovery services to help businesses recover data and services quickly in the event of failure.
- **Cloud Solutions:** Cloud 251 offers IaaS, SaaS, and PaaS services that allow businesses to scale and manage their IT resources efficiently.

- **Communication (Support) Mediums:** Phone support, email support, online ticketing and self-service portal and in person support.

What is the best cloud service model for banks?

The transition to cloud computing presents considerable challenges for banks, with security and regulatory compliance emerging as the most serious obstacles. The first priority is to protect the security and integrity of sensitive financial and personal data, as well as to ensure the resilience of mission-critical systems. Given the strict regulatory environment that governs the banking sector, any breakdown in security measures might have serious consequences. Banks cannot afford to underestimate the potential consequences connected with a security breach, which might jeopardize customer trust, incur heavy penalties, and inflict irreversible damage to their reputation (Sriram, 2011). Specific compliance standards require data segregation, which prohibits intermixing with other datasets on shared servers or databases. As a result, banks must retain a detailed grasp of where their data is located within the cloud architecture. This needs extensive data mapping and categorization processes to determine data residency and assure regulatory compliance. By precisely tracing the whereabouts of their data in the cloud, banks may limit the risk of noncompliance and protect the integrity of their regulatory requirements (Sriram, 2011).

While private clouds are well-known for providing the highest level of security among cloud options, it is worth noting that security can also be done successfully while reducing costs and meeting regulatory requirements by implementing local cloud solutions. Local cloud service providers are well positioned to handle high security needs, generally at a lower cost than other cloud deployment models. Furthermore, local cloud providers solve regulatory and compliance concerns, notably those requiring the separation of financial data from other information.

Given that certain compliance requirements prohibit the intermixing of financial data with other data, local cloud providers provide an appealing solution. Local cloud providers automatically comply with these rules because they store data in the same country as the bank. Furthermore, banks benefit from increased visibility and control over their data because they know exactly where it is housed within the local cloud architecture.

As a result, while private clouds excel in security, local cloud solutions provide a viable alternative that strikes a good balance between security, cost effectiveness, and regulatory compliance. Banks

can increase their confidence in the integrity and sovereignty of their data by leveraging local cloud services.

2.9 Related Works

The internal and external factors shaping the decisions of IT executives and experts regarding the adoption of cloud computing, with a specific focus on the Ethiopian banking sector (Bekele, 2014). The paper scrutinizes the influences on decision-making processes concerning cloud computing adoption, narrowing its scope to factors affecting these decisions and predominantly emphasizing international cloud service providers.

By concentrating on the Ethiopian banking sector, Bekele's research sheds light on the unique challenges and opportunities encountered by IT decision-makers within this specific industry context. The study aims to offer insights into the motivations, concerns, and considerations driving the adoption or reluctance towards cloud computing among Ethiopian banks. Furthermore, by focusing on international cloud service providers, the paper examines the external factors influencing decision-making, such as the reputation, reliability, security, and compliance offerings of these providers.

In the investigation conducted by (Solomon, 2017), the focus was on determining the most appropriate type of cloud service for banks in Ethiopia, with a particular emphasis on off-premise cloud service providers. The study concluded that a Hybrid cloud deployment model would be the most suitable option for Ethiopian banks, primarily due to concerns surrounding security.

Despite the recommendation of a Hybrid cloud approach, it is notable that the investigation did not specifically identify or consider local cloud service providers in Ethiopia. This omission is significant as local cloud service providers may offer unique advantages, including proximity to the banking institutions, enhanced regulatory compliance, and tailored services to meet local requirements.

The exploration of cloud computing readiness assessment among banks in Ethiopia is crucial for understanding their preparedness for cloud adoption. However, it is notable that in the assessment done by (Begna, 2017), the readiness of banks was primarily evaluated with a focus on international cloud service providers, without consideration for local service providers.

The absence of local service providers in the assessment may overlook potential advantages and challenges unique to the Ethiopian context. Local providers may offer localized expertise, cultural understanding, and specialized solutions tailored to the specific needs and challenges faced by banks in Ethiopia. Additionally, local providers may be better equipped to navigate regulatory requirements and address concerns related to data sovereignty and localization.

According to (Abere, 2014) a significant challenge faced by banks in Ethiopia is the processing of financial data abroad due to evolving financial regulatory requirements and security concerns associated with utilizing external public cloud service providers. To address this issue, Abere proposed the Ethiopian Banking Industries Hybrid Cloud (EBIHC) model, which integrates private and Ethiopian Banking Institutions (EBIs) clouds. In this model, each bank implements and manages its private cloud, while the EBIs cloud serves as a shared infrastructure.

However, Abere acknowledges that under the current model, banks remain responsible for the entire IT infrastructure, diverting their focus from core financial activities. To address this concern, Abere suggests a paradigm shift where banks relinquish responsibility for IT infrastructure to service providers, allowing them to concentrate solely on financial operations.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter outlines the methodologies employed in the research, encompassing several key This chapter explains the methodologies used for the research which includes a clear and specific research method that helps in reflecting the research question that guides the inquiry and reflects the purpose of the research, a description of the research design and approach that explains how the data will be collected, analyzed, and interpreted to answer the research question, a justification of the chosen methods and techniques that demonstrates their suitability and relevance for the research question and context, a description of the sampling strategy and criteria that shows how the participants or cases will be selected and why they are representative or informative for the research question, a description of the data collection methods and procedures that details what types of data will be gathered, how, when, where, and by whom, a description of the data analysis methods and procedures that outlines how the data will be organized, coded, categorized, and interpreted to identify patterns, themes, and meanings, a description of the ethical considerations and procedures that addresses the potential risks and benefits of the research, the informed consent process, the confidentiality and anonymity of the participants, and the data storage and security measures.

Research methodology is the structured approach used to tackle problems, essentially the science behind conducting research. It encompasses the systematic study of how research is conducted, outlining the procedures researchers employ to describe, explain, and predict phenomena. Research methodologies can be categorized into quantitative and qualitative methods. Quantitative methodologies involve measuring and analyzing numerical data to quantify relationships and patterns, while qualitative methodologies focus on understanding subjective experiences through techniques such as interviews and observations. Both quantitative and qualitative approaches offer unique strengths and are often combined to provide a comprehensive understanding of research questions. The choice of methodology depends on factors such as the research question, study population, and desired outcomes, ensuring the validity and rigor of research findings (Goundar, 2012a).

3.2 Research Approach

Research approaches are the strategic plans and procedures utilized throughout the research process to lead the journey from broad assumptions to the intricate processes of data collection, analysis, and interpretation. These approaches serve as road maps, detailing the path that researchers will take to conduct extensive and methodical inquiries into their chosen themes (Creswell, 2014).

Research can be divided into qualitative, quantitative and mixed methodologies based on the type of data sought. A mixed-method study combines the benefits of both methodologies.

Quantitative research is the practice of using numerical values derived from observations to explain and describe processes that the observations can reflect on. Qualitative research seeks to collect primary, firsthand textual data and evaluate it using certain interpretive methodologies. It is an effective strategy for examining a phenomenon with minimal available information because it is exploratory in character. Thus, the qualitative technique might reveal fresh insights, ideas, and produce novel theories (Taherdoost, 2022).

The quantitative method entails generating data in quantitative form that can be submitted to rigorous quantitative analysis in a formal and strict manner. Quantitative research relies on the measurement of quantity or amount. It applies to phenomena that can be stated quantitatively. Qualitative research, on the other hand, is concerned with qualitative phenomena, which are those that relate to or include quality or kind. Attitude or opinion research, which is aimed to find out how people feel or think about a certain issue or institution, is called qualitative research (Goundar, 2012b). Qualitative research is instrumental in uncovering the underlying meanings, patterns, and contexts of human behavior and experiences. It allows for a deeper understanding of complex phenomena and provides rich insights into various aspects of the subject under investigation.

Qualitative research offers several advantages, particularly in investigating sensitive and intricate situations, generating novel ideas and theories, and offering detailed descriptions of phenomena. By delving into the subjective perspectives and lived experiences of individuals, qualitative research enables researchers to gain a detailed understanding of the intricacies inherent in human behavior and interactions.

Mixed methods research is an approach to inquiry that involves gathering both quantitative and qualitative data, integrating the two types of data, and employing distinct designs that may include philosophical assumptions and theoretical frameworks (Creswell, 2014).

I have chosen to use qualitative research method for my study due to its effectiveness in exploring and comprehending a data that requires extra care and is confidential. Since I am dealing with financial data and a very sensitive information I found qualitative method suitable for my research. With the data gathered from management level representatives of each bank, cloud service providers in Ethiopia and NBE (National Bank of Ethiopia) which is the sole governor of banks in Ethiopia and INSA (Information Network Security Agency) which is the protector of the national interests of our country's information and information infrastructures. Qualitative research is instrumental in uncovering the underlying meanings, patterns, and contexts of human behavior and experiences. It allows for a deeper understanding of complex phenomena and provides rich insights into various aspects of the subject under investigation.

In my study, I intend to focus on exploring the challenges of local cloud service providers and banks in Ethiopia. By employing qualitative research methods, I aim to dig into the details of the services offered by local cloud service providers, the specific needs and requirements of banks in the Ethiopian, explore the security standard on data at rest and data in transit for banks and cloud service providers from INSA (Information Network Security Administration) and the rule makers and governing body for the banks in Ethiopia which is National Bank of Ethiopia (NBE). This approach enables me to examine the challenges, benefits, procedures, and other relevant factors associated with the adoption of cloud services in the banking sector.

3.3 Research design

This sector's complexity and the sensitive nature of the data involved necessitate a method that allows for an in-depth exploration of specific cases.

Overall, the qualitative research approach will facilitate a holistic understanding of the dynamics and complexities surrounding the adoption of cloud services in the banking sector in Ethiopia. By illuminating the challenges, benefits, and procedures involved, this study aims to contribute valuable insights to the existing body of knowledge and inform future research and practice in this area.

I have chosen to utilize a Case Study research design for this study because it is well-suited to capturing the essential information required for my research in the banking industry and cloud service providers in Ethiopia. This sector involves handling sensitive information, which can only be obtained from individuals occupying specific roles and divisions within the organization. The Case Study approach allows for an in-depth examination of these unique contexts and provides a

comprehensive understanding of the dynamics at play. By focusing on particular individuals and departments and by using semi-structured interviews, I have gathered detailed insights and perspectives that would be difficult to obtain through other research methods. This approach also enables me to explore the complex interactions and processes within the banking industry, offering a thorough analysis that addresses my research objectives. The richness of the data obtained through Case Studies will help to illuminate the specific challenges and opportunities faced by professionals in these critical positions, ultimately contributing to a more robust and informed understanding of the sector.

Through in-depth semi-structured interviews with representatives from NBE, INSA, cloud service providers and banks, I have gathered rich insights into their experiences, perspectives, and perceptions regarding cloud computing adoption.

Furthermore, this study explores the potential challenges faced by both banks and local cloud service providers should the adoption of local cloud services become a viable option. By identifying and analyzing these challenges, the research aims to provide insights into the barriers hindering the adoption of cloud services within the Ethiopian banking sector.

The research explores various aspects such as the regulatory environment, data security concerns, performance expectations, and cost considerations. Additionally, it examines the perceptions, attitudes, and readiness of banks towards embracing cloud technology, as well as the capabilities and offerings of local cloud service providers in meeting the unique needs and requirements of the banking industry.

Ultimately, the findings of this study aim to shed light on the complexities surrounding the adoption of cloud services by banks in Ethiopia and to provide recommendations for overcoming barriers and facilitating the transition towards cloud-based solutions.

3.4 Sampling Design

3.4.1 Sampling Method

I have chosen to use purposive sampling as my sampling method due to its effectiveness in selecting participants who have significant knowledge and profound insights into the realms of banking IT infrastructure and local cloud services. By intentionally selecting individuals with extensive experience in these domains, I aim to gather data that not only addresses my research questions but also encapsulates the broader perspectives prevalent within these fields. This method

allows me to prioritize depth and richness in the information obtained, ensuring that the insights collected from the study are comprehensive and reflective of the complexities inherent in the subject matter. By selecting participants who can provide in depth and detailed information, I aim to achieve a thorough understanding of the issues at hand and generate valuable insights that contribute meaningfully to the existing body of knowledge.

The research involves selecting a subset of banks and cloud service providers in Ethiopia to gather data for the study. The sampling strategy I have chosen is a type of Non-probability sampling which is purposive sampling, considering the sensitive nature of the information and the need to maintain confidentiality.

The selection criteria were twofold: first, the banks were chosen based on their age to capture insights from institutions with varying levels of maturity in IT infrastructure, operational strategies, and regulatory experience. This generational diversity ensures a broad understanding of the challenges and benefits of cloud adoption across different types of banks. Second, ease of data access was a key consideration. Banks with existing personal connections were prioritized to facilitate smoother data collection and ensure reliable and timely access to relevant information.
This approach provides a well-rounded perspective, combining insights from both established banks with extensive operational history and newer banks with more modern approaches. By doing so, the study aims to present a comprehensive analysis of the adoption of cloud services within the Ethiopian banking sector.

3.4.2 Sample Size

For the selection of banks in this study, a purposive sampling approach was adopted to ensure representation across different generations within the Ethiopian banking sector. Out of the 33 banks currently listed by the National Bank of Ethiopia, a sample of five banks were carefully selected to reflect diversity in terms of their years of establishment and their experience levels in the industry. The selected banks which are Awash Bank, Berhan Bank, Cooperative Bank of Oromia, Tsehay Bank, and Gada Bank represent a range from the oldest to the newest generation of banks.

Similarly, for cloud service providers, out of approximately 8 providers in Ethiopia, 4 are selected for the research. These providers are chosen based on their reputation, expertise, and willingness

to participate in the study. Given the confidentiality concerns, efforts are made to establish trust and ensure that the selected providers are willing to disclose relevant information for the research.

As a governing body NBE (National Bank of Ethiopia) and as a protector of the national interests of Ethiopia's information and information infrastructures, INSA (Information Network Security Administration) are included in the sample as a regulatory body.

By employing purposive sampling and ensuring confidentiality, the research aims to obtain valuable insights into the factors influencing the adoption of cloud services by banks in Ethiopia and the challenges faced by both banks and cloud service providers in this context.

3.5 Data Collection

3.5.1 Data Collection Methods

Among the various data collection methods available, including document review, observation, interview and focus group discussions, interview was chosen as the most suitable method for this study. This decision was made because the research area involves handling sensitive data, requiring a more personalized and secure approach to ensure participants feel comfortable sharing their insights.

Data collection involves interviews for primary data collection, and possibly document analysis for secondary data collection to gather insights from both banks and cloud service providers. The focus is on understanding the challenges, benefits, perceptions, and readiness for cloud adoption from both sides.

Interview

Out of the three types of interview techniques, structured interview where the questions are close ended, unstructured interview where the interview is conducted with an emerging questions from the interview guide with a more open-ended approach and semi-structured interview where the mix of the two approaches are used a semi-structured interview is chosen for this study.

Semi-structured interviews with key managerial position holders from chosen banks, representatives from local cloud service providers, officials from governing body (National Bank of Ethiopia) and INSA are used to acquire qualitative data. Participants are chosen based on their positions and expertise with cloud services for banks, ensuring that the information acquired is

relevant and useful. Interviews are recorded with the participants' permission and transcribed for analysis.

Qualitative researchers are not worried, and they rarely gather a large sample from the studied group. To put it simply, qualitative researchers select their cases gradually, without limiting the number of participants until the data has achieved saturation (Mohd Ishak & Abu Bakar, 2014). Though the banks and cloud service providers are selected with purposive sampling, participants from each organization are not limited in number.

I have collected data through semi-structured interview until my data is saturated which means I have collected my data to the point at which gathering additional data no longer provides new insights or themes relevant to the research questions. In qualitative research, such as studies using semi-structured interviews, reaching saturation is essential to ensure that the data collected is comprehensive and representative of the population or phenomenon being studied.

3.5.2 Data Collection Source

For primary data collection, semi structured interviews are conducted with higher officials responsible for the banks' IT infrastructure. These interviews focused on addressing the foundational questions of the research, providing insights into the decision-making process and challenges faced by banks regarding the adoption of cloud services, allowing for a comprehensive understanding of different perspectives and dimensions related to the research questions.

Secondary data is gathered from existing research studies, academic journals, and reports pertaining to banks and cloud service providers in Ethiopia. This secondary data provides valuable insights into the current state of the banking sector, trends in cloud adoption, challenges encountered, and best practices identified by previous researchers and industry experts. By synthesizing and analyzing this secondary data, the researcher benefited from a broader context and deeper understanding of the subject matter.

Overall, the combination of primary and secondary data collection methods allow for a comprehensive exploration of the research questions. The primary data obtained through interviews and questionnaires offer firsthand insights from key stakeholders, while the secondary data provided additional context and support for the findings and conclusions drawn from the

research. Through this approach, the research aims to generate valuable insights and contribute to the existing body of knowledge on cloud adoption in the Ethiopian banking sector.

I have collected both primary and secondary data from banks in Ethiopia and local cloud service providers to address the research questions effectively. Primary data is gathered through interviews, while secondary data is obtained from previous research studies, journals, and reports related to banks and cloud service providers in Ethiopia.

As the sole governing body for banks in Ethiopia officials from NBE (National Bank of Ethiopia) are interviewed to provide information regarding the rules and regulations regarding financial data management.

Since they are protectors of the national interests of our country's information and information infrastructures, officials from INSA (Information Network Security Administration) were also interviewed to reflect their idea on the specific Security standards that banks and cloud service providers should meet while dealing with financial data whether the data is at rest or in transit.

3.5.3 Data Collection Instrument

An interview guide was employed as the primary data collection instrument in this study to ensure the systematic gathering of relevant and detailed information. The guide was meticulously designed based on the conceptual framework, with questions thoughtfully drawn to align with the study's objectives and address the research questions comprehensively. By structuring the interview guide in this manner, it provided a clear framework for the interviews, enabling the researcher to delve deeply into key areas of interest while maintaining focus on the core themes. This approach ensured that the interviews elicited rich, in-depth responses, allowing for a nuanced understanding of the participants' perspectives and experiences relevant to the research topic. Additionally, I have used my phone as a recording device in order to record responses of the interviewee after getting the necessary permissions. Lastly the structured yet flexible nature of the interview guide allowed the me to inquiry further where necessary, uncovering valuable insights that contributed significantly to the overall findings of the study.

3.6 Data Analysis Techniques

Through the process of analysis, researchers can gain a new and insightful perspective on their data. This involves moving beyond initial descriptions to systematically breaking the data into

smaller components, examining how these elements are related, and ultimately developing a fresh understanding based on a reconceptualization of the data. By deconstructing the data, researchers classify it into categories, creating or applying concepts to organize these classifications. The connections established between these concepts form the foundation for constructing a renewed and more comprehensive description. At the heart of qualitative analysis are the interconnected processes of describing phenomena, categorizing them, and identifying relationships between concepts. This iterative process not only helps to illuminate the underlying structure of the data but also facilitates the development of nuanced interpretations and theories that provide deeper insights into the studied phenomena. It is through this detailed and reflective engagement with the data that researchers can move from surface-level observations to meaningful analytical conclusions (Dey, 2003).

Since I adopted a qualitative research method and collected data through in-depth interviews, I employed qualitative data analysis techniques to interpret and make sense of the information.

From some of the most common qualitative data analysis techniques like Thematic Analysis, Content Analysis, Narrative Analysis and Ground Theory I have used Thematic Analysis as the data analysis technique of my study. These techniques allowed me to systematically examine the responses, identify recurring themes, and explore patterns within the data. By focusing on the depth and richness of the participants' insights, I was able to gain a comprehensive understanding of the subject under study, ensuring that the analysis aligned closely with the qualitative nature of the research.

Thematic Analysis

Thematic analysis is a widely used qualitative data analysis method that was selected for this study to identify and analyze both pre-existing and emerging themes throughout the research process. This approach allows for a flexible and systematic examination of the data, enabling the researcher to uncover patterns and insights related to the challenges and benefits of adopting local cloud services in Ethiopian banks. By applying thematic analysis, the study ensures a thorough exploration of the data, allowing for a detailed understanding of the key factors influencing cloud adoption while accounting for new themes that arise during the analysis.

According to (Clarke & Braun, 2012) Thematic Analysis is a versatile method suitable for various research interests and theoretical perspectives. Its adaptability makes it an effective "basic" method for several reasons:

1. It accommodates diverse research questions, whether focused on people's experiences and understandings or the representation and construction of specific phenomena in different contexts.
2. It supports the analysis of various data types, including secondary sources like media and primary sources such as interview or focus group transcripts.
3. It is effective for both small and large datasets, ensuring flexibility in application.
4. It enables researchers to conduct data-driven analyses, grounded in the collected information, or theory-driven analyses, guided by existing theoretical frameworks.

This broad applicability makes Thematic Analysis a valuable tool for qualitative research.

The most significant difference across qualitative data analysis methods lies in how the data is coded. Coding serves as a way to identify recurring patterns, group related segments of data, and provoke deeper reflection on the meaning behind the data. By assigning codes to specific portions of text, researchers can organize their data and uncover key themes and concepts. However, the process of coding is not uniform and can vary greatly depending on the research approach and the nature of the data. Some methods might involve predefined codes based on theoretical concepts, while others might allow codes to emerge inductively as the researcher interacts with the data. This variability in coding techniques reflects the flexibility and depth inherent in qualitative analysis, where researchers can adapt their approach to best suit the complexities and nuances of their data (Kalpokaite & Radivojevic, 2019).

3.7 Ethical Considerations

Measures are taken to protect the confidentiality of the information obtained, adhering to ethical guidelines and regulations. To address the ethical issues I have used an official letter from Addis Ababa University School of Information Science Since banks and cloud service providers store and deal with a very sensitive financial data and confidential organizational information I have been cautious and careful with the information I request. And I made it clear for whoever was

sharing data that they are participating only for a study purpose and their identity will be confidential.

3.8 Credibility and Dependability

3.8.1 Credibility

In my research, I employed triangulation to ensure the credibility and of my findings. I gathered data from multiple sources, including in-depth interviews with banks, various local cloud service providers in Ethiopia, and two governing bodies.

Triangulation is often regarded as a hallmark of rigor in qualitative research. It involves collecting and analyzing data from multiple sources to obtain a more comprehensive understanding of the phenomenon under study. By integrating different perspectives, methods, or data types, triangulation enhances the credibility and depth of the research findings, ensuring that they are well-rounded and reflective of the complexity of the situation being investigated (Lacey, A., & Luff, 2009).

This approach allowed me to obtain diverse perspectives on the challenges and benefits of adopting local cloud services in Ethiopia. By comparing and cross-validating the data collected from these different stakeholders, I was able to achieve a more comprehensive and balanced understanding of the issues under investigation. Additionally, I systematically analyzed the data using a coding process within the TOE framework, further reinforcing the triangulation process by aligning the findings with established theoretical constructs.

3.8.2 Dependability

To ensure the validity of the study, the information collected from respondents was presented exactly as it was gathered, without any alterations or modifications. This approach maintains the authenticity and accuracy of the data, ensuring that the findings genuinely reflect the perspectives and experiences shared by the respondents. By adhering to this practice, the study upholds its credibility and reliability, providing a trustworthy foundation for analysis and conclusions.

I use validity in what I think is a fairly straightforward, commonsense way, to refer to the correctness or credibility of a description, conclusion, explanation, interpretation, or other sort of account. I think that this commonsense use of the term is consistent with the way it is generally used by qualitative researchers, and does not pose any serious philosophical problems. This use of

the term “validity” does not imply the existence of any “objective truth” to which an account can be compared. However, the idea of objective truth isn’t essential to a theory of validity that does what most researchers want it to do, which is to give them some grounds for distinguishing accounts that are credible from those that are not. Nor are you required to attain some ultimate truth for your study to be useful and believable (Maxwell, 1941).

CHAPTER FOUR

ANALYSIS, FINDINGS AND DISCUSSION

4.1 Introduction

This chapter presents the analysis and interpretation of the data collected from respondents through interviews. The primary purpose of the interviews was to explore and identify the challenges and benefits faced by both banks and local cloud service providers regarding the adoption of local cloud services by banks in Ethiopia. The findings aim to provide a comprehensive understanding of the key factors influencing this adoption process, shedding light on the opportunities and obstacles within the Ethiopian banking and cloud service sectors.

I have utilized the challenges and benefits of cloud computing identified in existing literature and integrated them into the TOE framework as codes. This approach allows for a detailed examination of the challenges and benefits faced by local cloud service providers and banks in Ethiopia. By aligning these predefined challenges and benefits within the framework, I can systematically explore their relevance and implications in the Ethiopian context, providing insights from both perspectives.

4.2 Analysis Instrument

The process of coding and re-coding qualitative data becomes significantly more efficient with the use of specialized computer software. These tools allow researchers to highlight small sections of text quickly and assign them to either pre-existing codes or new ones, all within seconds. Once coded, these data segments are systematically stored and can be easily searched and retrieved, much like browsing through organized documents. The researcher has the flexibility to assign custom titles and descriptions to each code, ensuring they align closely with the study's objectives. Furthermore, codes can be merged with others, divided into subcategories, or even arranged into more complex conceptual frameworks. This functionality facilitates the development of theoretical models, enabling researchers to organize and interpret their data more effectively and construct well-founded theories from their findings (Lacey, A., & Luff, 2009).

I used QDA Miner Lite software Version 2.0.9 for my qualitative data analysis, primarily because it is one of the free tools available for this purpose. Its accessibility and user-friendly interface

made it an ideal choice for organizing, coding, and interpreting qualitative data without incurring additional costs. The software's features, such as efficient coding, easy data retrieval, and the ability to manage large volumes of text, greatly supported my analytical process.

The research approach combines both inductive and deductive elements. It begins with the development of a conceptual framework, derived from a thorough literature review, which provides a structured foundation to guide data collection and analysis. However, this approach also maintains flexibility, allowing for unexpected insights or unanticipated information to emerge during the research process. This balance ensures that the study remains grounded in established knowledge while being open to discovering new perspectives and patterns within the data (Kalpokaite & Radivojevic, 2019).

4.3 Qualitative Data Analysis

The study employed a qualitative research method to achieve a deep understanding of the case, which involved gathering sensitive information from carefully selected representatives of banks, cloud service providers, and governing bodies. The findings are based on data collected from 12 representatives from banks spanning different generations, 4 representatives from local cloud service providers, and 3 representatives from governing bodies 2 from INSA and 1 from the National Bank of Ethiopia (NBE). All representatives hold higher or middle-level managerial positions, ensuring their insights are both strategic and operationally relevant. The findings are discussed as follows.

Qualitative data analysis is the systematic process of breaking down complex data into smaller, meaningful components to uncover its fundamental elements and structure. This method allows researchers to explore deeply into the nuances of the data, providing a clearer understanding of its underlying patterns and themes. Without a structured approach to analysis, researchers would have to rely solely on subjective impressions and intuitions about the data as a whole. While these intuitive insights can offer valuable perspectives, they are often insufficient for drawing comprehensive or reliable conclusions. By employing rigorous and logical analytical procedures, researchers can enhance the validity and depth of their findings, striking a balance between subjective interpretation and systematic examination (Dey, 2003).

This study utilized a qualitative research method, employing a case study approach to explore the topic in depth. Thematic analysis was applied to analyze the data systematically and derive meaningful insights, ensuring the research findings were well-structured and aligned with the objectives of the study.

The analysis is done by using the three concurrent flows of activity model: data reduction, data display, and conclusion drawing/verification by (Miles, M. B., & Huberman, 1994) .

Data Reduction

Data reduction is a critical process in qualitative research that involves selecting, focusing, simplifying, abstracting, and transforming raw data, which often come from field notes or transcriptions of interviews. It is an ongoing process that begins before data collection and continues through to the final reporting stage. Initially, data reduction occurs in the form of anticipatory decisions, where the researcher consciously or unconsciously selects a conceptual framework, determines the research questions, chooses cases for study, and decides on appropriate data collection methods. As the research progresses and data is collected, additional forms of data reduction take place. These include summarizing the data, coding it, identifying recurring themes, clustering related information, and making partitions of the data for more focused analysis. Researchers also engage in memo writing, which further refines their thinking and interpretation of the data. The process of data reduction continues even after fieldwork is complete, ensuring that only the most relevant and meaningful data remain to inform the final analysis and report. This iterative process allows researchers to manage the complexity of qualitative data, ensuring that it is systematically organized, focused, and transformed to address the research questions effectively (Miles, M. B., & Huberman, 1994).

In my research, I implemented a systematic data reduction process by using mixed coding method that includes both Deductive and Inductive coding to manage and analyze the collected qualitative data effectively. This began with anticipatory decisions during the planning phase, where I selected a conceptual framework, defined research questions, and identified appropriate cases and data collection methods while also paving a away for emerging codes.

As data collection progressed, I engaged in summarizing the data, coding it systematically, and identifying recurring themes aligned with the TOE framework. I clustered related information to uncover patterns and relationships within the data and wrote memos to refine my understanding and interpretation. This iterative process of data reduction continued beyond the fieldwork stage, ensuring that only the most relevant and meaningful data informed the final analysis and reporting. By focusing, simplifying, and organizing the data throughout the research, I was able to draw clear and insightful conclusions addressing the challenges and benefits of adopting local cloud services in Ethiopia.

Data Display

The second major flow of analysis work is data display. A display is an orderly, compacted compilation of information that allows for conclusion drawing and action. Looking at displays allows us to better grasp what is going on and take action based on that understanding. Throughout our work, we have come to believe that better displays are a significant step toward genuine qualitative analysis. This book covers a wide range of display types, including matrices, graphs, charts, and networks. All are intended to condense organized information into an easily accessible, compact form, allowing the analyst to understand what is going on and either reach justifiable conclusions or proceed to the next level of analysis suggested by the display. The production and use of displays, like data reduction, is integrated into analysis rather than independent from it. Analytic activities include designing a presentation, deciding on the rows and columns of a matrix for qualitative data, and determining which data, in which form, should be entered into the cells (Miles, M. B., & Huberman, 1994).

In my research, I employed data display as an integral part of the analysis process. By organizing and presenting the data in a structured and accessible format, I was able to facilitate a deeper understanding of the findings. Specifically, I used matrices to arrange the coded data systematically, aligning it with the TOE framework themes of technological, organizational, and environmental challenges and benefits of banks and cloud service providers in Ethiopia. These displays helped identify patterns, relationships, and trends within the data, providing clarity and direction for subsequent analysis.

The design of the displays was guided by the research objectives, involving decisions about the structure, such as rows and columns in the matrices, and the specific data to be included. This process not only aided in summarizing and organizing the data but also highlighted areas requiring further analysis. Through this iterative approach, data displays became a powerful tool in drawing meaningful conclusions and ensuring the validity of the qualitative analysis.

Conclusion Drawing and Verification

The third type of analysis activity is conclusion drawing and verification. From the commencement of data collection, the qualitative analyst begins to determine what things mean by identifying regularities, patterns, explanations, probable configurations, causal flows, and propositions. Data meanings must be examined for reliability, robustness, and "confirmability" (validity). Otherwise, we're left with intriguing stories about what happened, with uncertain truths and applications (Miles, M. B., & Huberman, 1994).

In my research, conclusion drawing and verification were essential steps in the analytical process. From the initial stages of data collection, I began identifying patterns, themes, and explanations within the data, guided by the TOE framework. This involved recognizing regularities and exploring potential causal relationships and configurations that connected the challenges and benefits of cloud adoption for banks and cloud service providers in Ethiopia.

To ensure the reliability and validity of these conclusions, I engaged in continuous verification. This process included cross-checking the data against emerging themes, revisiting the raw data to confirm interpretations, and triangulating findings from interviews with banks, cloud service providers, and governing bodies. I also critically assessed the robustness of the conclusions by seeking alternative explanations and considering the consistency of the findings across different data sources. Through this iterative approach, I ensured that the conclusions drawn were not only meaningful but also grounded in the data. This rigorous process strengthened the credibility and applicability of the research outcomes.

4.4 Findings

This section explains how the data collected and analyzed is used to answer the research questions. Below is a table explaining the participants of the study.

Participant Category	**Number of selected Organizations**	**Targets Organizations**	**Number of Participants**
Old generation Bank	1	Awash Bank	3
Middle generation Bank	2	Cooperative Bank of Oromia	2
		Berhan Bank	3
New generation Banks	2	Gada Bank	2
		Tsehay Bank	2
Local Cloud Service Providers	4	TeleCloud by Ethio Telecom	1
		Zergaw Cloud	1
		AACT (Alta-Africom Cloud Technology)	1
		Cloud 251	1
Governing Body	2	National Bank of Ethiopia	1
		INSA	1

Table 1: Demographics of participants

Since the analysis utilized the Technology-Organization-Environment (TOE) framework as the thematic structure, the findings will be discussed under each category. This approach enables a systematic identification of the technological, organizational, and environmental challenges and benefits experienced by banks and local cloud service providers. Furthermore, the themes used to identify the roles and responsibilities of governing bodies in addressing these challenges and promoting cloud adoption in Ethiopia will be discussed.

4.1.1 Benefits of Banks in Ethiopia

4.1.1.1 Technological Benefits of banks

This theme incorporates the codes discussed below to identify the benefits of banks from each code's point of view and all codes are merged to the technological benefits theme to identify the benefits of banks by using the TOE framework.

1. **Security and Data Protection**

Security is one of the most critical factors when banks consider adopting local cloud services. Many respondents from the banks emphasized that cloud services, when offered locally, could provide enhanced security features tailored to the specific needs of the Ethiopian banking environment. A high level manager at awash Bank highlighted, "By using local cloud services, we expect to have greater control over our security policies, which helps in protecting sensitive customer data in line with national regulations." The proximity of cloud service providers helps ensure faster responses to security threats. A mid-level manager from Berhan Bank added, "Local cloud providers understand the unique security requirements of Ethiopian banks, especially regarding data sovereignty, and have measures in place to safeguard against external cyber threats."

2. **Service Availability and Reliability**

Another critical technological benefit is the service availability and reliability that local cloud services can provide. Since local cloud providers are geographically closer to the banks, there is a lower risk of service disruption due to network latency or issues related to international data transfer. High level Manager at Coop Bank explained, "Local cloud providers offer more reliable services in terms of uptime because we don't have to rely on external providers. Any outages that might happen are dealt with locally, and response times are much quicker." Mid level Manager at Tsehay Bank said, "Having local cloud providers means we can expect greater availability and uptime since the infrastructure is closer, and technical support is more accessible, ensuring that our bank's online services run smoothly."

3. Cyber Crimes

In terms of cyber-crimes, adopting local cloud services can mitigate risks associated with external threats by providing advanced protection measures and security monitoring. A High level Manager at Gaada bank said, "Local providers offer better insights into the cyber-crime trends specific to the region, allowing for quicker intervention and more effective threat management." A Mid-level Manager at Awash Bank also noted, "The fact that local cloud providers are more familiar with the prevalent threats in the Ethiopian context makes it easier for them to implement the right cybersecurity measures to protect us from such crimes."

4. Legacy Systems and Integration

Local providers have the potential to simplify the integration of legacy systems into modern cloud environments. A Mid-level Manager at Awash bank mentioned, "Their familiarity with our current IT infrastructure allows them to create tailored solutions that minimize the challenges of migration." This capability would significantly reduce the cost and complexity of transitioning to the cloud. A Mid-level Manager at Berhan bank added, "Customized tools developed by local providers could ensure that our operations remain seamless and secure throughout the transition."

5. Flexibility

Banks value the operational flexibility that local cloud services could bring. As a High level Manager at Berhan bank stated, "Cloud solutions would enable us to adjust our capacity based on real-time demand, something we can’t easily do with on premise systems." This scalability would allow banks to respond efficiently to fluctuating customer needs, especially during periods of high demand. Moreover, tailored solutions from local providers would align better with the regulatory and operational constraints faced by Ethiopian banks.

6. Data Recovery

The ability of local cloud providers to offer robust data recovery solutions is seen as a significant benefit. A High level Manager at Coop bank highlighted, "Cloud-based backups ensure swift recovery of data in case of system failures, and while maintaining compliance with data residency

requirements." A Mid-level Manager at Awash bank also noted, "Having disaster recovery solutions within Ethiopia reduces the risk of permanent data loss and minimizes downtime, making our operations more resilient."

4.1.1.2 Organizational Benefits for Banks

This theme incorporates the codes discussed below to identify the benefits of banks from each code's point of view and all codes are merged to the organizational benefits theme to identify the benefits of banks by using the TOE framework.

1. **Vendor Lock-In:**

Local cloud providers are perceived to offer greater flexibility in vendor relationships compared to global providers. A High level Manager from Berhan bank stated, "Since local providers are bound by national regulations, they are more likely to ensure fairness in their contracts, reducing the risk of vendor lock-in." This creates an environment where banks feel less constrained by long-term commitments and more empowered to switch providers if services do not meet expectations. A Mid-level Manager from Awash bank also stated, "The competitive nature among local providers encourages them to maintain customer satisfaction and transparency, making vendor lock-in less of a concern."

2. **Cost Management**

The financial benefits of using local cloud services are highlighted by their potential to reduce operational costs. A Mid-level Manager from Awash bank explained, "Local providers can offer customized pricing models that better align with our budget constraints, unlike global providers who impose standard pricing structures." This flexibility allows banks to optimize spending without compromising service quality. Furthermore, A Mid-level Manager from Coop bank noted, "Cloud adoption would eliminate the need for large-scale investments in physical infrastructure, freeing up resources for other critical banking operations."

3. **Misunderstanding of Responsibilities**

Local providers are seen as better positioned to clarify the division of responsibilities in service agreements and open discussions to avoid misunderstanding of responsibilities between cloud service providers and banks in Ethiopia. A High level Manager from Coop bank stated, "Because they are based here, local providers can conduct more frequent and detailed discussions about roles and responsibilities, ensuring that there is no ambiguity." This transparency minimizes operational risks and helps banks maintain compliance. A Mid-level Manager at Berhan bank added, "Their closer proximity means that any misunderstandings can be resolved promptly, reducing delays and inefficiencies."

4.1.1.3 Environmental Benefits for Banks

This theme incorporates the two codes discussed below to identify the benefits of banks from each code's point of view and both codes are merged to the Environmental benefits theme to identify the benefits of banks by using the TOE framework.

1. **Regulatory Compliance**

Local cloud providers have a clear understanding of Ethiopian banking regulations, making them well-suited to help banks maintain compliance. A High level Manager from Awash bank stated, "By working with local providers, we can ensure that all our operations align with the directives of the National Bank of Ethiopia and INSA." This mitigates the risk of penalties and enhances trust between banks and regulatory authorities. Similarly, A Mid-level Manager from Berhan bank remarked, "Local providers' familiarity with the regulatory environment gives us confidence that we are not inadvertently violating any laws."

2. **Data Sovereignty and Residency**

Ensuring that data remains within Ethiopia's borders is a critical requirement for banks, and local providers play a pivotal role in fulfilling this mandate. A Mid-level Manager from Coop bank explained, "The ability to store sensitive financial data within the country ensures compliance with national laws and gives us control over our data." This sentiment was reinforced by A High level

Manager at Berhan bank, who said, "Knowing that our data is stored locally eliminates concerns about jurisdictional disputes or foreign interference."

4.1.2 Challenges of Banks in Ethiopia

4.1.2.1 Technological Challenges of banks

The theme of Technological Challenges was used across the responses, emphasizing various hurdles that banks in Ethiopia anticipate when considering the adoption of local cloud services. These challenges are categorized into six distinct codes: Security and Data Protection, Service Availability and Reliability, Cyber Crimes, Legacy Systems and Integration, Flexibility, and Data Recovery. Each of these codes reflects the participants' fear about the feasibility of cloud adoption under current circumstances.

1. **Security and Data Protection**

Participants consistently voiced concerns about the adequacy of security measures provided by local cloud providers to meet banking standards. A High-level Manager from Awash Bank stated, “Security is our top priority, but we are unsure if local providers can implement advanced measures to handle sensitive financial data.” This concern reflects the industry's heightened sensitivity toward securing customer data and preventing breaches. Similarly, A Mid-level Manager from Berhan Bank highlighted the risks of insider threats, mentioning, “We worry about whether local cloud providers can ensure their internal staff are fully vetted and capable of safeguarding data.” This suggests that trust in the personnel and processes of local providers is as critical as their technical security capabilities.

2. **Service Availability and Reliability**

Banks raised significant concerns about the reliability of local cloud infrastructure. A High-level Manager from Gaada Bank explained, “Uninterrupted service is crucial for banking operations, but frequent power outages and network disruptions in Ethiopia make us question the reliability of local providers.” This challenge underlines the dependency of banking operations on continuous system availability, which local cloud services must ensure. Moreover, A Mid-level Manager from Coop Bank noted, “Even if the provider guarantees uptime, the lack of redundancies in their

systems could lead to catastrophic failures." These responses underscore the participants' fear of over-reliance on potentially fragile infrastructure.

3. **Cyber Crimes**

The evolving threat landscape poses a serious challenge, as highlighted by multiple participants. A High-level Manager from Tsehay Bank remarked, "Cyber threats like ransomware and phishing are growing, and we're not convinced local providers have the expertise to counter these attacks." This sentiment reflects skepticism about whether local providers are sufficiently prepared to address advanced cyber threats. Adding to this concern, A Mid-level Manager from Awash Bank stated, "A successful attack on a shared platform could expose multiple banks at once, increasing the potential damage." This illustrates the banks' apprehension about multi-tenant environments, which could amplify vulnerabilities.

4. **Legacy Systems and Integration**

Integration of existing legacy systems with modern cloud solutions emerged as a key technological challenge. A Mid-level Manager from Berhan Bank mentioned, "Our systems are outdated and highly customized; transitioning to the cloud would require significant resources and expertise, which we currently lack." This highlights the complexity and cost implications of cloud migration for banks with legacy infrastructure. Additionally, A Mid-level Manager from Gaada Bank emphasized, "There's a lack of clarity on whether local providers can support seamless integration with our unique systems." This indicates the banks' need for reassurance on compatibility and smooth transition processes.

5. **Flexibility**

While flexibility is often cited as a benefit of cloud adoption, some participants viewed it as a challenge due to limited customization options provided by local cloud services. A High-level Manager from Coop Bank stated, "Cloud solutions need to be tailored to meet specific banking needs, but local providers seem to offer rigid, one-size-fits-all models." This rigidity could hinder banks from fully leveraging cloud technologies.

Furthermore, A Mid-level Manager from Awash Bank added, “The lack of scalable options from local providers limits our ability to adapt quickly to changing demands.” This perspective suggests that the scalability of local cloud solutions is a critical area of improvement.

6. **Data Recovery**

Concerns about disaster recovery and data restoration capabilities were frequently mentioned. A High-level Manager from Tsehay Bank noted, “The lack of tested and proven disaster recovery mechanisms from local providers makes us hesitant to adopt their services.” This indicates a gap in the confidence banks have in providers’ ability to handle data recovery during crises. Additionally, A Mid-level Manager from Berhan Bank stated, “We need assurance that our data can be recovered swiftly and completely in case of any failure.” This expectation underscores the importance of robust and reliable recovery solutions to mitigate operational disruptions.

4.1.2.2 Organizational Challenges for Banks

The theme of Organizational Challenges reflects the internal obstacles banks face when considering adopting local cloud services. This theme is comprised of three distinct codes: Vendor Lock-In, Cost Management, and Misunderstanding of Responsibilities. Each code reflects organizational concerns that could hinder the smooth transition to cloud adoption for Ethiopian banks.

1. **Vendor Lock-In**

A significant organizational concern expressed by several participants was the risk of becoming dependent on a single cloud provider. A Mid-level Manager from Coop Bank stated, “We are wary of becoming too reliant on a single cloud provider because switching providers down the line could be costly and complex.” This concern highlights the fear that long-term commitments with one cloud service provider could lead to operational inflexibility and excessive dependency on external vendors.

In agreement, A High-level Manager from Awash Bank remarked, “If we commit to a local cloud provider and later find better services elsewhere, migrating all our systems and data could be a

monumental task." The challenge of transitioning away from a vendor once integration with their platform is complete is a major organizational hurdle, as it would involve substantial time and resources.

2. Cost Management

Cost considerations emerged as a major barrier to cloud adoption, especially given the relatively high upfront costs associated with migrating to the cloud. A High-level Manager from Tsehay Bank mentioned, "The initial costs of moving to the cloud are high, and we're uncertain if the long-term savings will justify this investment." This reflects banks' concerns about the financial viability of cloud adoption, particularly in the face of high initial expenditures for migration and setup.

Similarly, A Mid-level Manager from Berhan Bank explained, "The cost of transitioning to local cloud providers, especially without clear data on long-term cost benefits, poses a significant challenge for us." This reflects the need for greater transparency in pricing models and a clear breakdown of expected costs before committing to a solution.

3. Misunderstanding of Responsibilities

The clarity around responsibilities between the bank and the cloud provider was another point of concern for several participants. A High-level Manager from Coop Bank noted, "We need a clear understanding of which responsibilities lie with us and which are the provider's, especially regarding data security and compliance." This shows that banks require well-defined service level agreements (SLAs) to ensure they understand the division of responsibility between themselves and the provider.

Furthermore, A Mid-level Manager from Gaada Bank added, "There is uncertainty about how much control we will retain over our data and systems when using local cloud services, and that's a major concern." This indicates that banks are cautious about the perceived loss of control over their data and operations when outsourcing to local cloud providers.

4.1.2.3 Environmental Challenges for Banks

The Environmental Challenges theme reflects the regulatory and external factors that could influence the decision to adopt local cloud services. This theme encompasses two codes: Regulatory Compliance and Data Sovereignty and Residency. These challenges stem from the complex regulatory landscape in Ethiopia, where local cloud adoption is affected by national laws and compliance requirements.

1. **Regulatory Compliance**

Regulatory compliance concerns were raised by several participants, who indicated that the regulatory framework for cloud services is still in development and might not fully support banking needs. A High-level Manager from Berhan Bank stated, “Local cloud providers need to be fully compliant with NBE’s regulations to ensure we meet the necessary legal standards.” This suggests that banks expect cloud providers to adhere to stringent national regulations regarding data security and service availability.

Similarly, A Mid-level Manager from Gaada Bank mentioned, “We’re concerned that without clear regulations guiding cloud service providers, we may inadvertently breach compliance standards.” This highlights the uncertainty that banks feel when it comes to understanding how their operations may be impacted by a rapidly evolving regulatory environment for cloud services in Ethiopia.

2. **Data Sovereignty and Residency**

Data sovereignty and residency concerns emerged as significant barriers to local cloud adoption. A Mid-level Manager from Tsehay Bank noted, “We are concerned that cloud providers could store sensitive data outside the country, which would violate data residency requirements and expose us to legal risks.” This concern reflects the fear that local cloud providers may not guarantee that data will remain within the country's borders, potentially violating national laws.

Additionally, A High-level Manager from Coop Bank remarked, “The issue of data sovereignty is critical because we cannot afford to let sensitive financial data be stored in foreign jurisdictions

where legal protections may not align with Ethiopian regulations." This underscores the need for clear data residency policies to ensure that the bank's data remains compliant with national sovereignty requirements.

4.1.3 Benefits of Local Cloud Service Providers

4.1.3.1 Technological Benefits for Local Cloud Service Providers

This theme encompasses the technological advantages that local cloud service providers offer, which can be critical in encouraging banks in Ethiopia to adopt cloud services. By evaluating the responses from each provider, we can understand how their technological offerings position them as viable partners for the banking sector in Ethiopia. Below, I will explain how each code under "Technological Benefits" contributes to this theme, integrating responses from the local cloud service providers.

1. **Security and Data Protection**

Security and data protection are paramount for local cloud service providers, especially in the banking sector. Local cloud providers ensure that sensitive financial data is protected from breaches, cybercrimes, and unauthorized access. A representative from Telecloud stated, "Security is a top priority, and we implement strong encryption mechanisms for both data-at-rest and data-in-transit. We use multi-layered firewalls, access controls, and intrusion detection systems." Telecloud emphasizes robust encryption and layered security strategies to protect data, making it a strong technological benefit that aligns with the stringent data protection requirements of the banking sector.

Cloud 251 also focuses on security, stating, "We provide real-time monitoring, Advanced threat detection, and automated incident response mechanisms to protect banks from cyber-crimes." This use of advanced tools highlights Cloud 251's proactive approach to cybersecurity, ensuring the continuous protection of sensitive banking information and mitigating emerging threats.

These responses demonstrate that local cloud providers use advanced security technologies to offer banks the confidence they need regarding the safety of their data, which is a critical technological benefit.

2. **Service Availability and Reliability**

For banks, ensuring that cloud services remain available without interruption is crucial. Local cloud service providers understand this need and have built reliable infrastructure to support high service uptime.

A representative from AACT mentioned, "Our cloud platform is designed for high availability, using geo-redundant data centers and automated load balancing to ensure services remain operational even during unexpected outages." AACT's focus on geo-redundancy and automated balancing systems helps ensure that banking services are always accessible, which is an essential technological benefit for banks that rely on constant service availability.

Additionally, Zergaw Cloud stated, "We offer a service level agreement (SLA) guaranteeing uptime and support availability." Their SLAs serve as an added assurance, reinforcing the commitment to providing reliable cloud services to their banking clients. These efforts in ensuring service availability and reliability are pivotal in fostering trust among banks, enabling them to consider local cloud services as viable solutions for their IT infrastructure.

3. **Cyber Crimes**

Cybercrime is a growing concern for cloud service providers worldwide, especially in sectors dealing with sensitive financial data. Local cloud service providers have made strides in implementing technologies to prevent and respond to cyber threats.

A representative from Cloud 251 stated, "A significant challenge is educating bank staff about common cyber threats like phishing and social engineering, which require more than just technological solutions to mitigate." This acknowledgment shows that while Cloud 251 emphasizes security technology, they also recognize the importance of human factors in preventing cybercrime, integrating both educational initiatives and advanced tech tools to combat threats.

AACT also highlighted their technological capabilities, stating, "We leverage advanced machine learning and smart tools to detect and respond to cyber threats in real-time." This use of machine learning and smart tools reflects AACT's commitment to using cutting-edge technologies to

protect against and respond to cybercriminal activities, which is a technological benefit that provides a competitive edge.

By leveraging smart tools and machine learning, local cloud providers ensure that they stay ahead of cybercriminals, which is a critical advantage when dealing with financial data.

4. **Legacy Systems and Integration**

Many Ethiopian banks rely on legacy systems that need to be integrated with modern cloud solutions. Local cloud service providers that can bridge this gap provide significant value to the banking sector by ensuring that traditional systems work seamlessly with the cloud.

A representative from Telecloud explained, "Our team conducts a detailed assessment of the bank's existing IT infrastructure and legacy systems before migrating them to our cloud. We provide customized integration solutions and APIs that allow for seamless communication between legacy systems and our cloud infrastructure." Telecloud's commitment to providing tailored integration solutions makes them a valuable partner for banks looking to migrate to the cloud without losing functionality.

Zergaw Cloud resonated a similar approach, stating, "We offer customized integration solutions and APIs to ensure that our cloud environment works seamlessly with the bank's existing infrastructure." Zergaw Cloud's ability to tailor their cloud solutions to the specific needs of banks further enhances their technological appeal, offering a smooth transition from legacy systems to cloud-based services.

These integration capabilities ensure that local cloud providers can support banks in the modernization of their IT infrastructure, which is a crucial benefit in today's digital banking environment.

5. **Flexibility**

Flexibility in cloud services is key for banks, as their needs evolve with market changes. Local cloud service providers that offer scalable and adaptable services position themselves as long-term partners for banks.

A representative from AACT highlighted, "Our cloud solutions are designed for flexibility, allowing banks to quickly scale resources in response to growing demand or new projects." This ability to scale resources based on demand ensures that banks can adjust their IT infrastructure according to their evolving business needs, a significant technological benefit for any institution.

Cloud 251 further emphasized flexibility, stating, "Our solutions allow banks to easily scale their IT infrastructure based on demand." The ability to quickly scale resources provides flexibility for banks, ensuring that they only use the resources they need, optimizing cost and efficiency.

Flexibility in cloud services allows banks to adapt quickly to changing business requirements, making it a key technological benefit for local cloud providers.

6. **Data Recovery**

Data recovery is a crucial aspect of cloud services, especially for banks that cannot afford to lose critical financial data. Local cloud providers that offer strong data recovery solutions provide a much-needed technological benefit to banks.

Telecloud explained, "We provide comprehensive backup solutions, including real-time data replication across multiple sites." This feature ensures that in the event of a disaster, data is immediately available, which minimizes the risk of prolonged downtime for banks.

Zergaw Cloud also offered reassurance in this area, stating, "We offer disaster recovery solutions and backup systems that can restore data rapidly after an incident." Their disaster recovery solutions ensure that banks can recover quickly and avoid disruptions to their services.

These data recovery capabilities are an essential technological benefit, providing banks with peace of mind knowing that their data can be restored quickly in the event of an incident.

4.1.3.2 Organizational Benefits for Local Cloud Service Providers

This theme explores how local cloud service providers offer organizational advantages that enhance their ability to deliver services to Ethiopian banks. These benefits are crucial in convincing banks to adopt cloud services, as they address concerns about cost management, vendor

lock-in, and clarity of responsibilities. Below is a detailed explanation of the organizational benefits, categorized by specific codes.

1. Vendor Lock-In

One significant organizational benefit offered by local cloud providers is their approach to mitigating concerns about vendor lock-in. Unlike international providers, local providers emphasize flexibility and transparency in service agreements.

A representative from Telecloud highlighted, "We provide our clients with the option to move their data and services to other platforms without additional costs or unnecessary complexities." This ensures banks can transition smoothly between providers, reducing their fear of dependency on a single vendor.

Similarly, Cloud 251 explained, "We use open standards and interoperable platforms, ensuring that banks are not restricted to our services alone." By prioritizing open standards, Cloud 251 demonstrates its commitment to avoiding vendor lock-in, providing banks with the freedom to adapt their IT strategies without long-term constraints.

These efforts to prevent vendor lock-in make local providers appealing partners for banks, offering the flexibility to explore multiple service options.

2. Cost Management

Cost management is another area where local cloud providers excel, offering competitive pricing and cost-efficient solutions tailored to the needs of Ethiopian banks.

Zergaw Cloud emphasized, "We structure our pricing based on the specific requirements of each client, ensuring they pay only for what they use." This pay-as-you-go pricing model allows banks to optimize their spending by scaling resources up or down as needed, making cloud services more financially viable.

AACT shared a similar perspective, stating, "We offer affordable service packages designed specifically for the financial sector, reducing the cost burden of maintaining on-premises

infrastructure." By tailoring services for the banking sector, AACT helps banks reduce overheads while accessing advanced IT capabilities.

Cost management is a significant organizational benefit that local cloud providers bring, enabling banks to achieve IT modernization without incurring prohibitive expenses.

3. Misunderstanding of Responsibilities

Local cloud providers have taken proactive measures to clarify roles and responsibilities in cloud service agreements, ensuring smoother collaborations with banks.

A representative from Cloud 251 noted, "We work closely with banks to establish clear terms in our contracts, explicitly defining the responsibilities of both parties regarding data management and system security." This approach minimizes confusion and builds trust between providers and banks, fostering better partnerships.

Telecloud further elaborated, "Our onboarding process includes detailed training sessions for bank IT teams, ensuring they fully understand the shared responsibilities in a cloud environment." This focus on education ensures that banks are well-informed about their role in managing cloud services, reducing the risk of operational misunderstandings.

By addressing the potential for misunderstandings early, local cloud providers enhance the effectiveness of their partnerships with banks, building a foundation of mutual trust and accountability.

4.1.3.3 Environmental Benefits for Local Cloud Service Providers

This theme explores the environmental advantages that local cloud service providers bring to Ethiopian banks. These benefits address regulatory compliance and concerns about data sovereignty and residency, two critical considerations for banks operating in Ethiopia. Below is a detailed analysis of the environmental benefits, categorized by specific codes and supported by responses from the providers.

1. Regulatory Compliance

Local cloud providers have shown their commitment to complying with Ethiopian regulations, making their services more appealing to banks constrained by strict policies. Telecloud emphasized, "We ensure that our systems align with local regulations and work closely with stakeholders to adapt to any new compliance requirements." By staying ahead of regulatory expectations, Telecloud builds confidence among potential banking clients.

A representative from Zergaw Cloud stated, "Our services are designed to meet Ethiopian financial sector standards, and we provide full transparency in our compliance processes." This proactive approach ensures that banks feel secure in outsourcing their IT needs to providers who respect local governance. Although NBE currently restricts cloud adoption for banks, local providers have positioned themselves as compliant partners, ready to support banks when regulations allow.

2. Data Sovereignty and Residency

Data sovereignty and residency are major concerns for Ethiopian banks, given the need to store sensitive information within national borders. Local cloud providers offer a significant advantage in this area.

Cloud 251 highlighted, "Our data centers are fully located within Ethiopia, ensuring that client data never leaves the country." This commitment to keeping data local helps banks meet regulatory requirements while maintaining control over their information.

Similarly, AACT added, "We prioritize data residency to ensure that banks retain ownership and governance over their data in compliance with Ethiopian laws." This focus on sovereignty alleviates banks' fears of losing control over sensitive financial information, positioning local providers as secure and reliable partners.

By guaranteeing local data residency, providers like Cloud 251 and AACT address one of the most critical environmental concerns for Ethiopian banks, ensuring regulatory alignment and client confidence.

4.1.4 Challenges of Local Cloud Service Providers

This section explores the challenges faced by local cloud service providers in Ethiopia, categorized into technological, organizational, and environmental themes. The analysis reflects the influence of the National Bank of Ethiopia's (NBE) prohibition on cloud adoption by banks and the absence of specific security standards or penalties from the Information Network Security Agency (INSA). Insights are derived from representatives of Telecloud, Zergaw Cloud, Cloud 251, and AACT.

4.1.4.1 Technological Challenges

Technological challenges faced by local cloud service providers include the complexities of building and maintaining secure, reliable, and scalable infrastructure tailored to the banking sector. These challenges are amplified by regulatory restrictions, such as the prohibition on cloud adoption by the NBE, and the lack of specific security standards or penalties from INSA. The theme focuses on issues such as ensuring security and data protection, service reliability, mitigating cyber threats, integrating with legacy systems, enabling flexibility, and implementing effective disaster recovery strategies.

1. **Security and Data Protection**

The lack of specific security standards from INSA adds to the complexity of ensuring robust data protection for banks. Providers must rely on general best practices without clear national benchmarks.

A representative from **Cloud 251** explained, "Without specific guidelines or penalties for non-compliance, we are left to interpret global standards and align them with the expectations of potential banking clients." This uncertainty increases the difficulty of meeting stringent security demands.

AACT highlighted, "Even though we follow industry best practices, the absence of concrete national security frameworks limits our ability to reassure banks about the adequacy of our security measures."

2. Service Availability and Reliability

Infrastructure limitations in Ethiopia, compounded by the NBE's prohibition on cloud adoption, deter investments in infrastructure improvements tailored to banking needs.

Telecloud stated, "We have invested in redundant systems to ensure availability, but with banks unable to use our services, scaling these investments becomes challenging."

Zergaw Cloud added, "The regulatory environment prevents us from showcasing our reliability to banks, which could otherwise benefit from cloud scalability and uptime guarantees."

3. Cyber Crimes

The absence of specific penalties for security breaches places a heavier burden on providers to self-regulate while addressing rising cybercrime.

AACT noted, "We are committed to preventing attacks like ransomware, but without an overarching regulatory framework or support, our efforts are not backed by enforceable penalties or incentives."

4. Legacy Systems and Integration

Integration with legacy systems remains a major challenge, further complicated by the lack of regulatory support encouraging modernization.

Zergaw Cloud stated, "Banks rely heavily on outdated systems, and with cloud adoption restricted, there’s little motivation for them to modernize or explore integration solutions."

5. Flexibility

While cloud solutions are inherently flexible, limited adoption by banks makes it harder to refine services tailored to specific banking needs.

Cloud 251 remarked, "Banks’ reluctance to adopt cloud services due to regulatory barriers stifles innovation in offering more customizable solutions."

6. **Data Recovery**

Developing robust disaster recovery plans is challenging without active collaboration with banks, which is hindered by the NBE's prohibition on cloud usage.

AACT observed, "Our disaster recovery systems are capable, but without direct involvement from banks, aligning recovery processes with their needs is speculative at best."

4.1.4.2 Organizational Challenges

Organizational challenges stem from internal and external factors that affect how cloud service providers operate. These include managing perceptions around vendor lock-in, balancing the high costs of maintaining cutting-edge infrastructure with limited demand, and addressing misunderstandings about shared responsibilities in cloud service models.

1. **Vendor Lock-In**

The prohibition on cloud adoption by NBE creates a perception of risk among banks, even when providers emphasize open standards. **Telecloud** mentioned, "Banks are wary of vendor lock-in, and the regulatory stance on cloud services reinforces their hesitation, making it harder for us to demonstrate our flexibility."

2. **Cost Management**

Balancing the cost of maintaining infrastructure with limited demand is a key challenge, as regulatory barriers prevent banks from engaging with local cloud providers.

Zergaw Cloud stated, "Without bank clients, the cost of maintaining cutting-edge infrastructure becomes increasingly difficult to justify."

3. **Misunderstanding of Responsibilities**

The absence of specific standards from INSA adds to the confusion about shared responsibility models, leaving banks uncertain about their role in cloud environments.

Cloud 251 highlighted, "Banks often assume that the provider handles everything, but without clear regulations or awareness programs, these misunderstandings persist."

4.1.4.3 Environmental Challenges

Environmental challenges involve the broader regulatory and legal landscape within which local cloud service providers operate. This includes navigating compliance requirements, addressing data sovereignty and residency concerns, and managing external pressures.

1. **Regulatory Compliance**

The NBE's prohibition on cloud adoption by banks creates a fundamental barrier to service delivery. Additionally, INSA's lack of specific security standards leaves providers navigating compliance ambiguities.

Telecloud emphasized, "The absence of clear regulatory frameworks makes it difficult to convince banks of our readiness, even though we comply with global standards."

2. **Data Sovereignty and Residency**

While local providers comply with Ethiopian data residency laws, the NBE's restriction on cloud adoption nullifies the advantages of local sovereignty.

Zergaw Cloud noted, "We ensure data remains within Ethiopia, but with banks unable to use our services, this compliance advantage goes unutilized."

4.1.5 Role of Regulatory Body

As the primary regulatory authorities overseeing the banking sector in Ethiopia, INSA and NBE share many responsibilities in ensuring the successful adoption of local cloud services by banks. Although their roles differ slightly, both organizations contribute significantly to the regulatory framework. The category "Role of Governing Body" examines how INSA and NBE collectively define and shape the standards for cloud adoption, particularly focusing on security, compliance, and risk management. Since NBE currently does not allow banks to utilize cloud services, this partnership primarily concerns the development of future frameworks that will guide the secure

use of cloud technologies. The codes under each theme have been merged, representing the collaborative approach of INSA and NBE as the regulatory bodies for Ethiopia's banking sector.

In the Role of Regulatory Body category, I focused on how the governing bodies, namely INSA (Information Network Security Agency) and the NBE (National Bank of Ethiopia), contribute to or influence local cloud adoption by banks in Ethiopia. This category assesses their roles in ensuring that cloud services are secure, compliant with regulations, and properly monitored, as well as how they guide and manage risks associated with adopting cloud technologies in the banking sector by merging the codes used for the study in to themes like Cybersecurity and Data Protection Standards, Regulatory Compliance and Risk Management, Auditing and Monitoring Mechanisms and Cloud Adoption and Future Directions.

4.1.5.1 Cybersecurity and Data Protection Standards

This theme examines the roles of INSA and the NBE in ensuring that banks' cloud adoption aligns with national cybersecurity and data protection standards. It focuses on the importance of protecting sensitive banking data against cyber threats and ensuring compliance with privacy regulations. The theme evaluates the agencies' responsibility in setting guidelines for data protection, mitigating cybersecurity risks, and monitoring the overall security environment in cloud services used by banks.

1. **INSA - Cybersecurity Audits**

INSA does not proactively conduct audits on local cloud service providers but only does so upon request, whether by banks or local cloud service providers. The audits focus on assessing the security maturity of the cloud services and identifying any vulnerabilities.

A High level Manager from INSA noted: "At the moment, we do not conduct regular audits unless requested by NBE, the banks or the cloud service providers. Our role is to assess the security maturity of the cloud systems and ensure that any vulnerabilities are addressed. It is up to the banks to request these audits before they adopt cloud services provided by local cloud service providers."

A Mid- level Manager from INSA noted: “If a bank or cloud provider requests an audit, we check for security controls like data encryption and access management. We help identify any gaps in cybersecurity, but it’s important to note that we don’t initiate these audits independently.”

2. **INSA - Cyber Threat Mitigation**

INSA emphasizes the need for cloud service providers to adopt measures to protect against emerging cyber threats, including ransomware, phishing, and insider threats. They encourage implementing robust threat detection and mitigation strategies but only if requested to assess cloud providers. A High level Manager from INSA noted: “Though we don't impose direct requirements on cloud providers at this stage, we encourage them to have strong cybersecurity practices, such as threat detection systems and incident response plans, especially against cyber threats like ransomware and phishing. These systems should be in place before any bank considers adopting cloud solutions.”

3. **NBE – Data Protection Standards**

NBE is in the process of developing data protection guidelines for cloud adoption but currently lacks any formal regulations for cloud services. These standards will ensure sensitive banking data is protected, once cloud adoption is permitted.

NBE Representative noted: “Currently, we do not have any regulations for cloud adoption, whether for local or international cloud service providers. However, we are in the process of developing data protection directives that will be applicable once cloud adoption is allowed. These will ensure that sensitive banking data is protected, especially with respect to the regulations we have for traditional banking data.”

4.1.5.2 Regulatory Compliance and Risk Management

This theme explores how INSA and NBE manage regulatory compliance and risk factors associated with cloud adoption. It includes assessing the risks for data protection, ensuring compliance with national laws, and setting up processes for future cloud adoption.

1. **INSA - Compliance Gaps**

INSA does not yet conduct proactive assessments of compliance gaps but will identify these issues upon request. Banks and cloud service providers need to address compliance gaps as part of their cloud adoption process.

A High level Manager from INSA noted: "Currently, we do not regularly assess compliance gaps and risk management on local cloud service providers. Our role is to step in when requested, especially when banks or cloud providers need an audit to ensure compliance with local laws and risk measures in place".

A Mid-level Manager from INSA: "When we are asked to evaluate a provider or a bank, we look for compliance with national regulations, such as those related to cybersecurity and data protection. If gaps are found, we provide recommendations, but we don't conduct routine checks."

2. **NBE - Risk Management in Cloud Adoption**

NBE is not yet allowing banks to adopt cloud services. Once cloud adoption is approved, NBE will expect banks to have a solid risk management framework in place, especially concerning data protection, cybersecurity, and disaster recovery.

A High level Manager from NBE noted: "Currently, no banks are using cloud services as we do not allow it. However, once cloud adoption is approved, we will expect banks to implement a comprehensive risk management framework. This will include data protection measures, risk assessment strategies, and a disaster recovery plan to ensure business continuity. It's critical for banks to be prepared for the risks associated with cloud computing."

4.1.5.3 Auditing and Monitoring Mechanisms

This theme addresses the roles of INSA and NBE in auditing and monitoring cloud service providers. It explores the processes and responsibilities for ensuring compliance and assessing security once cloud adoption is approved.

1. **INSA – Cloud Provider Security Assessment**

INSA only conducts security assessments of cloud providers when requested by banks or providers. This includes evaluating the security posture of cloud providers and ensuring that they meet the necessary standards.

A High level Manager from INSA noted: “We do not proactively assess cloud providers but respond to requests from banks or providers themselves. When we are asked, we evaluate the security infrastructure and ensure that they meet the basic standards of cybersecurity and compliance. However, this is only done on an ad-hoc basis.”

A Mid-level Manager from INSA noted: “Cloud security assessments are important, but they only occur when a bank or cloud provider requests them. Our role is to ensure that the cloud provider’s security framework aligns with national standards, but this is not something we initiate unless explicitly asked.”

2. **NBE – Cloud Provider Approval Process**

Since NBE does not currently allow cloud adoption, there is no active approval process. However, once cloud adoption is permitted, NBE will establish a formal process to evaluate and approve cloud providers.

A High level Manager from NBE noted: “At this stage, we do not have an approval process because no banks are allowed to use cloud services. However, once we allow cloud adoption, we will establish an evaluation process. This process will ensure that only cloud providers who meet our security, compliance, and operational standards will be approved for use by banks.”

4.1.5.4 Cloud Adoption and Future Directions

This theme looks forward to the eventual adoption of cloud services by the banking sector and how INSA and NBE will guide this process. It discusses the future regulatory framework, the approval process, and the innovations that could be encouraged as part of cloud adoption.

1. **INSA - Cloud Security Innovations**

INSA encourages local cloud providers to innovate in terms of security, using advanced technologies like advanced threat detection, block chain, and enhanced encryption. However, these are only suggestions since INSA does not enforce such measures at this point.

A High level Manager from INSA noted: “We encourage local cloud providers to explore advanced security solutions like advanced threat detection and blockchain to ensure that the data is secure. However, we are not imposing these technologies at the moment. The banking sector will benefit greatly if local providers can integrate such innovative solutions into their cloud services and we hope that providers take these technologies into account as they build their infrastructure.”

2. **NBE - Cloud Adoption Plans**

NBE does not currently allow cloud adoption, but it is developing guidelines and frameworks to facilitate secure adoption in the future. These will cover regulatory requirements, data protection, and risk management.

A High level Manager from NBE noted: “Currently, we are not allowing banks to adopt cloud services, but we are in the process of developing comprehensive guidelines for cloud adoption. These guidelines will address data protection, security standards, and risk management frameworks to ensure that the adoption is done securely once we approve it.”

3. **NBE - Non-Compliance Penalties**

Since NBE currently doesn’t allow banks to use cloud services, there are no non-compliance set but once cloud adoption is allowed, NBE will implement penalties for non-compliance, such as financial fines or service provider disqualification, to ensure that both banks and cloud providers follow the required regulations.

A High level Manager from NBE noted: “If any bank or cloud provider fails to meet our regulations once cloud services are allowed, there will be penalties. These could include fines or

the removal of approval for service providers. It is crucial that both banks and providers comply with the standards to ensure the security of banking operations."

4.5 Discussion

This section is structured in alignment with the TOE Framework, drawing on the findings discussed in Chapter Four. It is organized to address the research questions comprehensively and to establish connections between these findings and the insights from prior studies reviewed in Chapter Two. By doing so, this section aims to provide a cohesive analysis that integrates the study's results with the existing body of knowledge, highlighting both consistencies and contrasts with earlier research.

To answer the research question 1 (RQ1) the challenges and benefits of banks in Ethiopia in order to adopt cloud services provided by cloud service providers in Ethiopia is discussed by using the TOE framework.

4.5.1 Benefits of Ethiopian Banks in Adopting Local Cloud Services

The potential benefits for Ethiopian banks in adopting cloud services from local cloud service providers are promising, particularly when considering the unique dynamics of the Ethiopian banking industry. While no bank is currently utilizing local cloud services due to regulatory constraints, the presence of these providers within the country presents a strategic advantage. Below is a conclusive analysis of these potential benefits:

1. Technological Benefits

Local cloud service providers have an intrinsic understanding of the Ethiopian banking sector's technical needs, which positions them to deliver tailored solutions effectively.

- **Security and Data Protection**: Providers operating in Ethiopia are more likely to align their services with local security requirements. This understanding reduces the complexity of integrating services that meet stringent data protection and cybersecurity standards.
- **Service Availability and Reliability**: Banks in Ethiopia often grapple with infrastructure challenges, but the localized presence of cloud providers ensures high availability and low latency, which are critical for seamless banking operations.

- **Cybersecurity**: Ethiopian cloud providers are better equipped to anticipate region-specific cyber threats, offering solutions that cater specifically to the local banking ecosystem's vulnerabilities.
- **Flexibility and Data Recovery**: Local providers can offer highly customizable solutions for backup and disaster recovery plans, tailored to the operational patterns and compliance needs of Ethiopian banks.

2. Organizational Benefits

Engaging with local cloud service providers could help Ethiopian banks navigate organizational challenges while gaining strategic advantages.

- **Vendor Lock-In**: Unlike foreign providers, local providers can offer more flexible contracts and operational models. Ethiopian banks would have greater bargaining power and easier access to support.
- **Cost Management**: Transitioning to a local cloud provider could lead to substantial cost savings in the long term. Customizable service packages mean banks can scale their usage efficiently without overcommitting resources.
- **Understanding Responsibilities**: Local providers are more accessible for consultations and collaborations, making it easier for banks to clarify shared responsibilities and ensure smooth operations.

3. Environmental Benefits

The regulatory and operational landscape of Ethiopia plays a significant role in shaping the potential benefits of local cloud services.

- **Regulatory Compliance**: Local providers are well-versed in the mandates of the National Bank of Ethiopia (NBE) and can tailor their services to ensure compliance. This eliminates the need for banks to navigate foreign compliance standards, which may not align with local regulations.
- **Data Sovereignty and Residency**: The assurance that sensitive banking data remains within Ethiopian borders is a key benefit. Local providers operate within Ethiopia's legal

framework, giving banks peace of mind about the storage and processing of critical financial information.

4.5.2 Challenges of Ethiopian Banks in Adopting Local Cloud Services

The potential challenges Ethiopian banks face when considering the adoption of local cloud services stem from a variety of technological, organizational, and environmental factors. These reflect not only the current limitations within the Ethiopian context but also broader concerns about transitioning to cloud-based operations in the banking sector.

1. Technological Challenges

Local cloud service providers, while situated within Ethiopia and offering potential proximity advantages, present significant technological challenges to banks.

- **Security and Data Protection**: Banks are apprehensive about whether local providers can meet the rigorous security demands required to safeguard sensitive financial data. Concerns revolve around providers' ability to deploy advanced and up-to-date security measures to mitigate cyber threats.
- **Service Availability and Reliability**: Unstable infrastructure in Ethiopia, including frequent power outages and unreliable internet connectivity, raises questions about the consistency and dependability of cloud-based operations. Even with local providers, these challenges persist and could disrupt banking services.
- **Cyber Crimes**: The relatively limited exposure of local providers to global cybersecurity practices may leave them vulnerable to sophisticated attacks, such as ransomware and insider threats. Banks are particularly concerned about the ability of these providers to preemptively identify and mitigate such risks.
- **Legacy Systems and Integration**: Many Ethiopian banks operate with outdated legacy systems that are deeply embedded in their operations. Transitioning these systems to the cloud or integrating them with modern platforms presents a risk of operational disruptions and compatibility issues.
- **Flexibility and Scalability**: While local cloud providers promise enhanced flexibility, banks remain uncertain about whether these providers have the capacity to scale their

services effectively to accommodate the growth and evolving needs of the banking industry.

- **Data Recovery**: The preparedness of local providers in implementing robust data recovery mechanisms in case of data loss or cyber incidents remains a concern. Banks require assurances that data can be restored quickly and accurately without significant downtime.

2. Organizational Challenges

Organizational challenges stem from the internal processes and financial considerations of banks, as well as their relationships with service providers.

- **Vendor Lock-In**: Dependency on a single provider poses a significant risk for banks, particularly if the provider fails to deliver or ceases operations. Banks fear that switching providers could involve high costs and operational delays.
- **Cost Management**: Although local cloud services are often promoted as cost-efficient, banks are wary of unforeseen expenses associated with transitioning, maintaining, and scaling services.
- **Misunderstanding of Responsibilities**: Ambiguity in service-level agreements between banks and providers could lead to gaps in accountability. Banks are concerned that unclear delineation of responsibilities might result in service disruptions or unmet expectations.

3. Environmental Challenges

External regulatory and contextual factors also play a significant role in hindering the adoption of local cloud services by banks.

- **Regulatory Compliance**: The National Bank of Ethiopia imposes stringent regulations that currently prevent banks from adopting cloud services. Even if allowed, banks would require detailed guidance to navigate compliance requirements and avoid potential penalties.
- **Data Sovereignty and Residency**: Maintaining control over data within Ethiopia is a critical requirement for banks. However, there are concerns about the transparency of data

storage practices among local providers, as well as their ability to ensure data residency compliance.

To support the study a visual representation of the study is provided below on Fig 1.

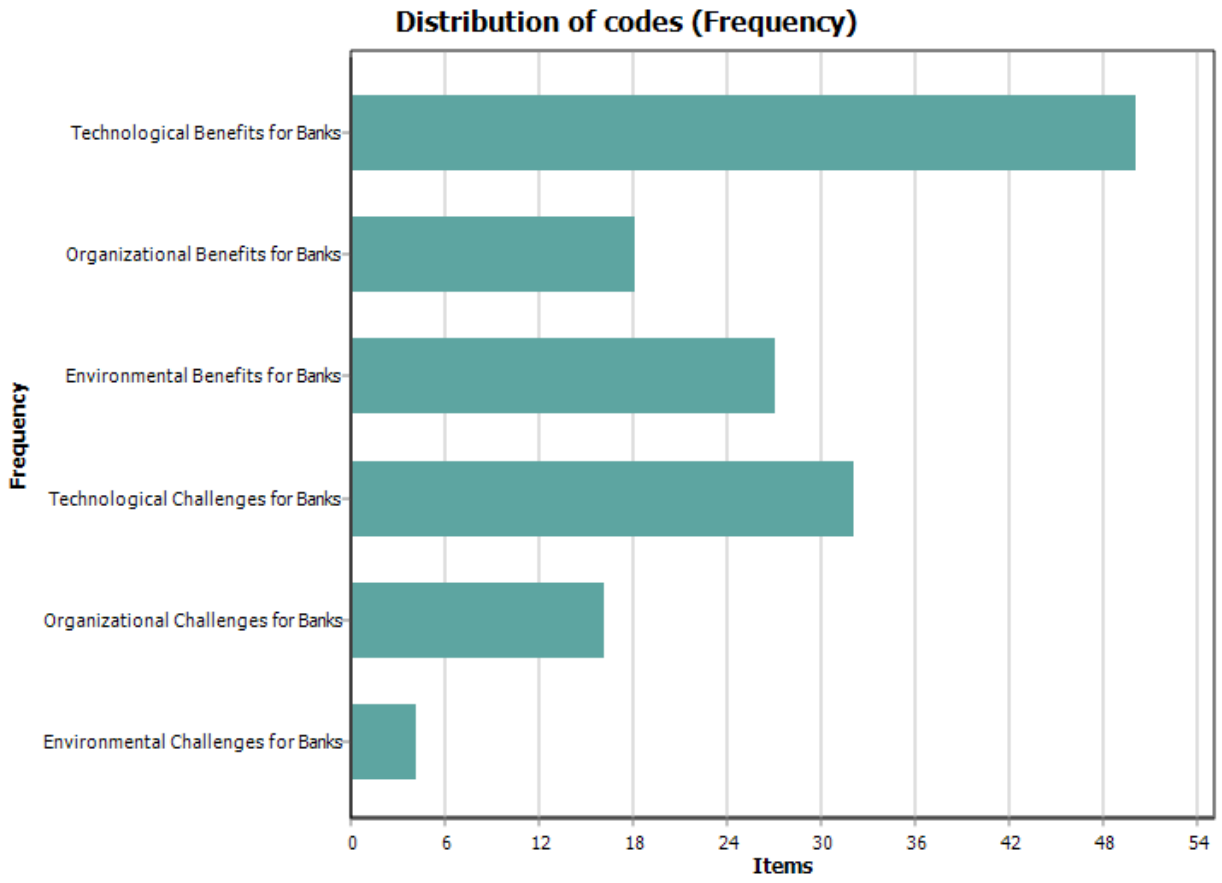

Figure 2: Challenges and Benefits of Banks

As we can see in the graph a higher frequency is shown on the benefits for banks under each category compared to the categories under challenges of banks which indicates the higher the frequency the higher the number of significant information is connected to the codes under these themes.

To answer research question two (RQ2) Challenges and Benefits of Local cloud service providers in order to provide their services to the banking sector in Ethiopia is discussed using the TOE framework.

4.5.3 Benefits of Local Cloud Services for Banks in Ethiopia

Local cloud service providers are well-equipped to ease the adoption of cloud services for banks in Ethiopia, addressing key operational, technological, and compliance challenges while enhancing efficiency and reliability. These benefits are categorized into technological, organizational, and environmental themes, demonstrating how cloud solutions can modernize banking operation.

1. Technological Benefits

Local cloud service providers in Ethiopia are uniquely positioned to understand and address the specific technological needs of Ethiopian banks. Being embedded in the local context, these providers have an in-depth understanding of the banking sector's requirements, allowing them to deliver tailored solutions that meet the unique challenges banks face:

- **Security and Data Protection:** Local providers are well-aware of the security challenges Ethiopian banks encounter, such as regulatory requirements and emerging cyber threats. They offer customized protection measures, including encryption tailored to local compliance needs and additional layers of security designed to address sector-specific vulnerabilities. This localized approach ensures Ethiopian banks receive protection that aligns with their operational realities.
- **Service Availability and Reliability:** Providers' proximity enables them to design and manage infrastructure that meets the reliability expectations of Ethiopian banks. By offering redundancy within local data centers and rapid response to issues, they ensure uninterrupted services, which is crucial for banking operations reliant on real-time processing.
- **Cyber Crimes:** Understanding the evolving threat landscape in Ethiopia, local providers develop specialized tools and systems to combat cybercrimes such as ransomware and insider threats. Their familiarity with regional cyberattack trends allows them to offer preemptive security measures that are both effective and relevant.
- **Legacy Systems and Integration:** Many Ethiopian banks still operate legacy systems that require careful integration into modern platforms. Local providers bring expertise in

bridging these systems with cloud technologies, offering solutions that minimize disruptions and support gradual modernization.

- **Flexibility and Data Recovery:** By tailoring scalable solutions to the specific needs of Ethiopian banks, local providers enable them to adjust IT resources dynamically, ensuring cost efficiency and operational flexibility. Additionally, localized disaster recovery mechanisms ensure rapid restoration of services with minimal impact on operations, a critical need in the banking sector.

2. Organizational Benefits

Cloud adoption simplifies operational management and reduces costs for banks:

- **Vendor Lock-In:** Providers address concerns of dependency by offering flexible migration options and supporting hybrid solutions, allowing banks to maintain control over their IT strategy.
- **Cost Management:** The shift from capital expenditure (CAPEX) to operational expenditure (OPEX) reduces upfront investments and aligns costs with actual usage, making IT spending more predictable.
- **Misunderstanding of Responsibilities:** Local providers actively support banks by offering clear role definitions, training, and guidance, ensuring seamless operations and effective management of cloud services.

3. Environmental Benefits

Local cloud providers align with national compliance requirements, facilitating secure and lawful operations:

- **Regulatory Compliance:** Providers demonstrate readiness to support compliance monitoring, enabling banks to adhere to national and international standards. This ensures that cloud adoption aligns with legal and regulatory expectations.
- **Data Sovereignty and Residency:** Onshore storage and processing of banking data align with Ethiopian laws, enhancing trust and ensuring that sensitive data remains within national borders, reducing risks associated with cross-border data management.

4.5.4 Challenges of Local Cloud Service Providers

Local cloud service providers face a range of challenges under technological, organizational, and environmental themes.

1. Technological Challenges

- **Security and Data Protection:** Providers struggle to meet robust security requirements without specific standards or penalties from INSA, limiting banks' confidence in cloud solutions.
- **Service Availability and Reliability:** High availability demands costly investments in infrastructure, which is unsustainable given NBE's restrictions on cloud adoption.
- **Cyber Crimes:** Evolving cyber threats require significant resources to address, while INSA's lack of guidelines leaves providers without a benchmark.
- **Legacy Systems and Integration:** Integrating with outdated banking systems is complex, increasing costs and operational hurdles.
- **Flexibility and Data Recovery:** Providers face challenges delivering scalable, resilient solutions without significant investments in disaster recovery infrastructure, which banks currently cannot utilize.

2. Organizational Challenges

- **Vendor Lock-In:** Banks' concerns over limited flexibility and migration options deter interest in cloud adoption, requiring providers to develop open-standard solutions.
- **Cost Management:** High operational costs, combined with suppressed demand due to regulatory restrictions, hinder competitive pricing.
- **Misunderstanding of Responsibilities:** Banks often misconstrue their roles in shared security responsibilities, creating gaps in service delivery readiness.

3. Environmental Challenges

- **Regulatory Compliance:** The NBE's prohibition on cloud adoption is the most significant challenge, effectively preventing providers from engaging with banks.

- **Data Sovereignty and Residency:** While local providers align with residency laws, the lack of specific compliance guidance from INSA undermines their ability to leverage this advantage.

To support the study a visual representation of the study is provided below on Fig 2.

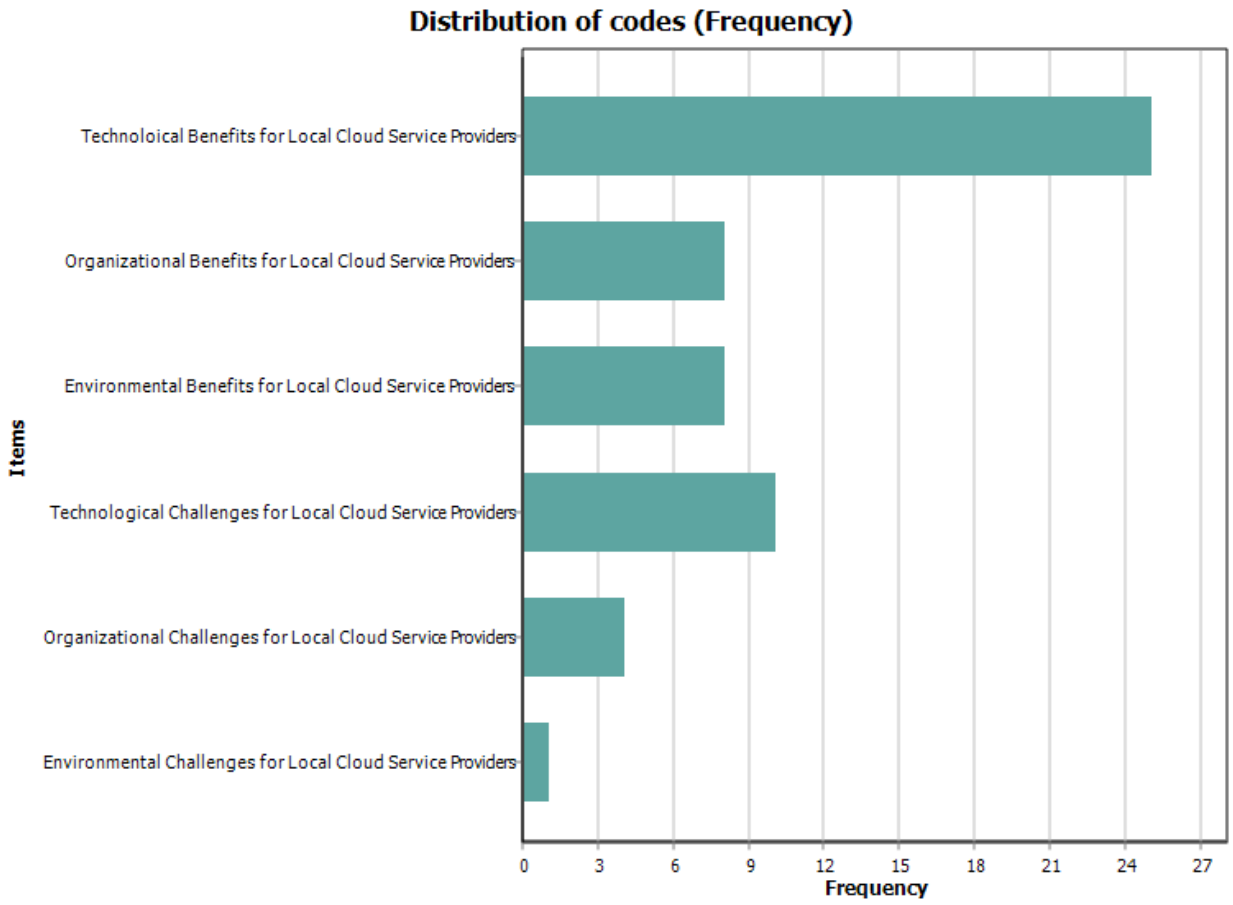

Figure 3: Challenges and Benefits of Local cloud service providers

As we can see in the graph a higher frequency is shown on the benefits for local Cloud Service providers under each theme compared to the theme under challenges of local Cloud Service providers which indicates the higher the frequency the higher the number of significant information is connected to the codes under these themes.

The Last category which immerged during the study which wasn't the part of the TOE framework will be discussed bellows as it has its own themes and codes that immerged during the study.

4.5.5 Roles of Regulatory Body

The roles of INSA and NBE as the regulatory body will be discussed here

1. Cybersecurity and Data Protection Standards

Both INSA and NBE share a major concern about cybersecurity and data protection standards for local cloud services. Currently, INSA does not have specific standards for cloud providers, and it only conducts audits upon request, which means there is no proactive framework for ensuring the security of cloud services. NBE, on the other hand, does not allow banks to adopt cloud services at all, so the need for clearly defined cybersecurity and data protection guidelines is not yet urgent. However, both institutions recognize the importance of secure services for protecting sensitive banking data.

- **Data Protection Standards:** INSA and NBE emphasize the importance of data protection, but neither body has formalized regulations or requirements regarding cloud adoption. NBE's position of restricting cloud services for banks, particularly around issues such as data residency, results in a delay in enforcing security measures for the cloud. INSA's role in providing audits upon request indicates a reactive approach rather than a proactive regulatory framework for ensuring data protection.
- **Cybersecurity Oversight:** Both INSA and NBE are concerned about the security of banking data, particularly in the context of emerging cyber threats such as ransomware, data breaches, and insider attacks. While NBE doesn't permit banks to use cloud services, INSA's limited capacity to perform audits highlights a need for more robust cybersecurity mechanisms and standards for cloud providers, especially in a potential future scenario where cloud services might be adopted.

2. Regulatory Compliance and Risk Management

The primary concern under this theme is the absence of clear regulatory compliance and risk management frameworks to guide the adoption of cloud services for banks. Both NBE and INSA are focused on ensuring that banks comply with national and international regulations, but there is a lack of guidance regarding cloud-specific compliance requirements.

- **Compliance Monitoring:** While NBE currently focuses on auditing traditional banking infrastructure, it does not have a clear framework for assessing cloud service providers' compliance with security and privacy regulations. This lack of clear directives may hinder banks from being able to demonstrate compliance when they eventually adopt cloud services. Similarly, INSA, which conducts audits only upon request, highlights the need for regular, systematic audits for cloud service providers to monitor their compliance with national security standards.
- **Risk Management in Cloud Adoption:** NBE and INSA both recognize the risks associated with cloud adoption. NBE does not allow cloud adoption, limiting banks' exposure to potential risks. However, NBE has outlined its expectation for banks to follow rigorous risk management practices for their traditional infrastructures. Once cloud adoption becomes permissible, NBE will need to establish specific risk management requirements to ensure that banks are adequately prepared for the risks involved in the transition to cloud environments.

3. Auditing and Monitoring Mechanisms

Both INSA and NBE understand the need for robust auditing and monitoring mechanisms to ensure the security and integrity of banking data. However, both institutions face challenges due to the absence of a standardized, proactive approach to cloud services.

- **Cybersecurity Audits:** INSA's limited capacity to perform audits only when requested means that its role in monitoring the security of cloud services is reactive. This could result in vulnerabilities going unnoticed until they are specifically flagged by stakeholders. NBE's prohibition on cloud services further diminishes the need for an active auditing framework for cloud providers, although NBE does conduct regular audits on banks' existing infrastructure.
- **Cloud Provider Approval Process:** NBE's lack of a structured process for evaluating cloud providers presents a significant concern, especially if cloud adoption is allowed in the future. Banks will need a clear and reliable process for selecting cloud service providers who meet regulatory standards for data protection and security. In the absence of this, the adoption of cloud services could create new security risks and compliance issues.

4. Cloud Adoption and Future Directions

The adoption of cloud services in the banking sector is still uncertain due to the absence of regulations and a restrictive stance from NBE. However, both INSA and NBE recognize that once cloud adoption is allowed, the future direction of local cloud services will need to be carefully managed to ensure both security and compliance.

- **Cloud Security Innovations:** INSA, in particular, has acknowledged the need for cloud providers to adopt more advanced security innovations, such as advanced threat detection and blockchain, to better protect banking data. However, this cannot happen until the regulatory environment for cloud adoption is clearer and more formalized.
- **Cloud Adoption and Future Directions:** NBE's reluctance to allow banks to adopt cloud services places a limitation on the banking sector's ability to explore the full benefits of cloud computing. When the NBE revises its stance, there will be concerns about how banks can transition safely to the cloud, ensuring that their data remains secure, their compliance requirements are met, and the risks associated with cloud adoption are effectively mitigated.

To support the study a visual representation is provided below on Fig 3.

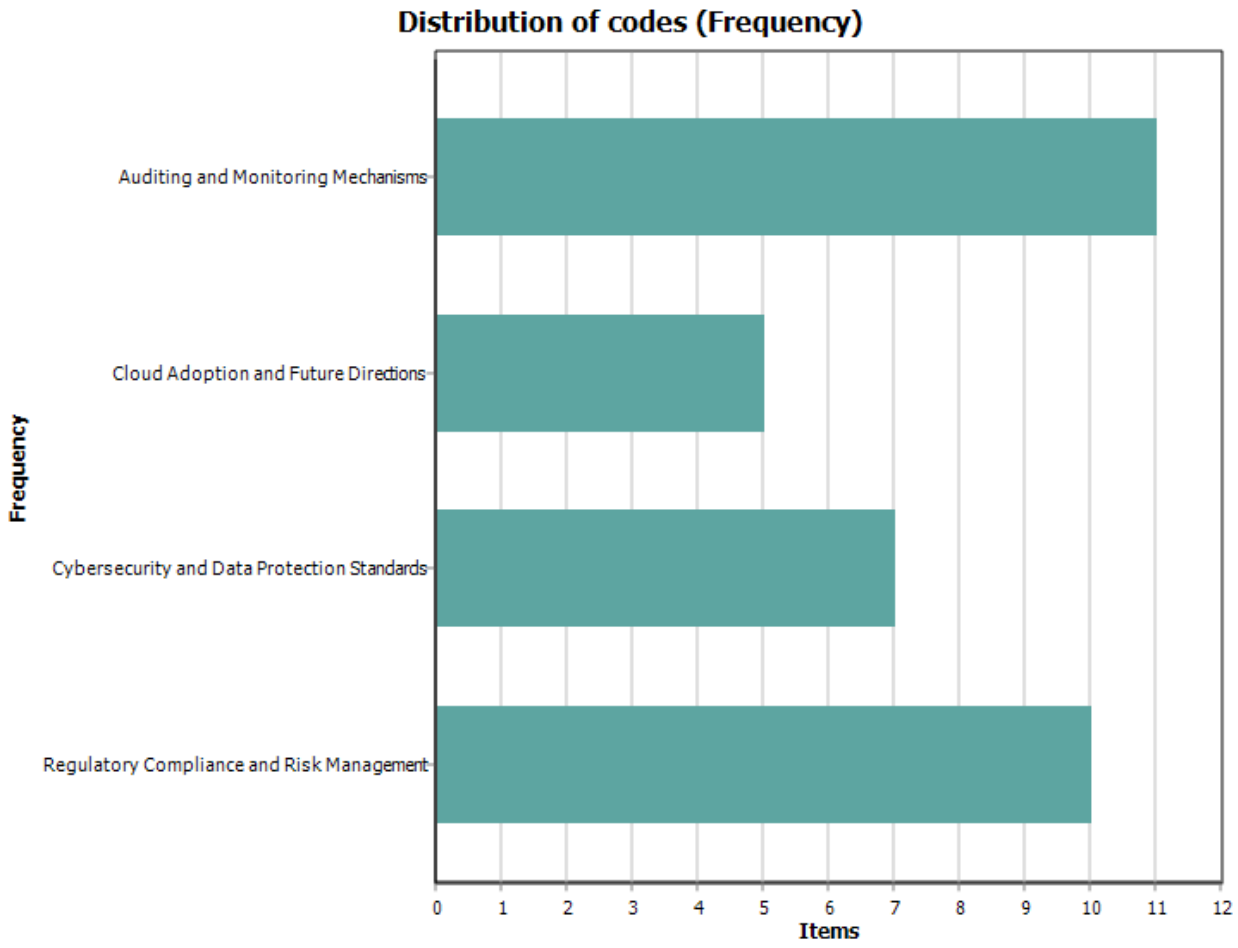

Figure 4: Roles of regulatory body

As we can see on the figure the themes under the regulatory body are shown with their corresponding frequencies, which shows which themes have the highest number of significant information coded to them.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

5.1 Conclusion

In conclusion, this study has provided valuable insights into the challenges and benefits of Ethiopian banks adopting local cloud services, as well as the obstacles faced by local cloud service providers in delivering these services. The findings indicate that while banks are cautiously optimistic about cloud adoption, significant regulatory and technological barriers hinder the progress where the study answered the first research question. Local cloud providers have the potential to enhance operational efficiency, reduce costs, and offer tailored solutions that align with the unique needs of Ethiopian banks. However, the absence of clear regulatory standards from INSA and the National Bank of Ethiopia's (NBE) prohibition on cloud adoption remain critical roadblocks preventing banks from fully leveraging these advantages that revealed the challenges faced by banks which answered the first research questions.

To answer the first research question the study also highlights the key benefits banks can gain once regulatory challenges are addressed. Cloud adoption would enable scalable, secure, and cost-effective IT solutions, allowing banks to shift their focus to core financial operations while ensuring compliance and data security. Furthermore, aligning technological, organizational, and environmental factors through collaboration with cloud providers can enhance banks' competitiveness and resilience in a rapidly evolving financial landscape.

From the perspective of local cloud service providers, the research reveals that they face difficulties related to regulatory uncertainty, security concerns, and a lack of trust from banks. Without an established regulatory framework, providers struggle to prove their reliability and compliance with international security standards which answers the second research question. This creates hesitation among banks, further delaying cloud adoption. Addressing these challenges will require stronger partnerships between banks, cloud providers, and regulatory bodies to develop clear policies, improve security mechanisms, and build confidence in local cloud services.

Ultimately, this study has answered its core research questions by demonstrating that while cloud adoption presents numerous benefits, it also requires overcoming significant regulatory, technological, and organizational challenges. Achieving a secure and sustainable cloud ecosystem for Ethiopian banks will depend on proactive collaboration among all stakeholders to create a supportive regulatory framework and ensure the smooth transition to cloud-based services.

5.2Recommendation

To facilitate secure cloud adoption, regulatory bodies like INSA and NBE should establish clear cloud adoption standards. Banks should collaborate with local cloud providers to build trust by ensuring robust security measures and compliance with national regulations. Local cloud providers need to focus on robust security and data protection tailored to meet the banking sector's needs. Clear service agreements must be established between banks and providers to define roles, SLAs, and responsibilities. Banks should also invest in ongoing training to overcome cultural and organizational barriers to cloud adoption. Lastly, continuous dialogue among banks, providers, and regulators is essential for developing tailored cloud solutions that support the sector’s growth.

For Future work

- Researchers can develop a security framework for local cloud service adoption by banks.
- Researchers can investigate what exactly the governing body’s concern is to allow banks to use local cloud services.
- Impact of local Cloud Adoption on Customer Experience and Competitive Advantage.

Reference

AACTS. (2024). *AACTS*. https://www.aacts.cloud/

Abere, A. (2014). *A Cloud Computing Framework for Ethiopian Banking Industry*. *10*(May).

Achuthan, S. (2019). *Cloud Computing For Banks – Benefits and Challenges* (Vol. 10, Issue 3). http://www.ijser.org

Amini, M., & Javid, N. J. (2023). A multi-perspective framework established on diffusion of innovation (DOI) theory and technology, organization and environment (TOE) framework Toward Supply Chain Management System Based on Cloud Computing Technology for Small and Medium Enterprises. *Organization and Environment …*, *11*(8). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4340207%0A

B. Patel, P. H., & Kansara, P. N. (2021). Cloud Computing Deployment Models: A Comparative Study. *International Journal of Innovative Research in Computer Science & Technology*, *9*(2), 45–50. https://doi.org/10.21276/ijircst.2021.9.2.8

Begna, L. (2017). *Cloud Computing Readiness Assessment for banking sector in Ethiopia*.

Bejju, A. (n.d.). Cloud Computing for Banking and Investment Services. *Advances in Economics and Business Management (AEBM, Volume 1*. https://www.researchgate.net/publication/296839704_Cloud_Computing_for_Banking_and_Investment_Services

Bekele, S. (2014). *Exploring Factors That Affect the Decision to Adopt Cloud Computing Technology in Ethiopian Banking Sector* (Vol. 17, Issue 3). http://etd.aau.edu.et/handle/123456789/14725

Bhardwaj, S., Jain, L., & Jain, S. (2010). Cloud Computing : a Study of Infrastructure As a Service (Iaas). *International Journal of Engineering*, *2*(1), 60–63. http://ijeit.org/index_files/vol2no1/CLOUD COMPUTING A STUDY OF.pdf

Clarke, V., & Braun, V. (2012). Thematic Coding and Analysis. *Teaching Thematic Analysis: Overcoming Challenges and Developing Strategies for Effective Learning*. https://doi.org/10.4135/9781412963909.n451

Cloud251. (2024). *Cloud251*. https://www.cloud251.com/

Creswell, J. W. (2014). The Selection of a Research Approach. *Research Design*, 3–23. https://doi.org/45593:01

de Bruin, B., & Floridi, L. (2017). The Ethics of Cloud Computing. *Science and Engineering Ethics*, *23*(1), 21–39. https://doi.org/10.1007/s11948-016-9759-0

Dennis, & Ravi, A. (2019). The Crucial Challenges Faced By the Banking Sector on Adopting Cloud Computing. *International Journal of Research in Advent Technology (IJRAT) Special Issue*, *4*(5), 51–53.

Dey, I. (2003). Qualitative data analysis: A user-friendly guide for social scientists. In *Qualitative Data Analysis: A User-Friendly Guide for Social Scientists*. https://doi.org/10.4324/9780203412497

Dwivedi, Y. K., Wade, M. R., & Schneberger, S. L. (2012). Informations Systems Theory: Vol.2. *Springer*, *28*(May), 461. https://doi.org/10.1007/978-1-4419-6108-2

Erturk, E. (2021). *A Critical Inquiry : Using TOE as a Theoretical Framework for Digital Inclusion Beyond 2021*. *March*. https://doi.org/10.13140/RG.2.2.36111.71844

Ethio telecom. (2024). *Telecloud*. https://telecloud.ethiotelecom.et

Everett M. Rogers, Arvind Singhal, M. M. Q. (2008). *An Integrated Approach to Communication Theory and Research* (2nd Editio). https://www.taylorfrancis.com/chapters/edit/10.4324/9780203887011-36/diffusion-innovations-everett-rogers-arvind-singhal-margaret-quinlan

Goundar, S. (2012a). *Cloud Computing*. https://www.researchgate.net/publication/333015026_Chapter_3_-_Research_Methodology_and_Research_Method

Goundar, S. (2012b). What are Different Research Approaches? Comprehensive Review of Qualitative, Quantitative, and Mixed Method Research, Their Applications, Types, and Limitations. *Journal of Management Science & Engineering Research*, *March 2012*, 1–43. https://www.researchgate.net/publication/333015026_Chapter_3_-_Research_Methodology_and_Research_Method/comments

Hailu, D. (2020). Cloud Computing Adoption Challenge in Case of Commercial Bank of Ethiopia. *International Journal of Development Research*, *10*(01), 33562–33465. https://www.researchgate.net/publication/340084301

Hajizadeh, P., & Hajizadeh, A. (2020). Benefits and Challenges of Cloud Computing for Financial Sector. *International Journal of Academic Accounting*, *4*(5), 73–79. www.ijeais.org/ijaafmr

Joe, T. (2023). Cloud Computing and Information Systems: Enabling Scalability and Flexibility. *Business Studies Journal* , *15*(3), 1–3. https://www.abacademies.org/articles/cloud-computing-and-information-systems-enabling-scalability-and-flexibility.pdf

Kalpokaite, N., & Radivojevic, I. (2019). Demystifying qualitative data analysis for novice qualitative researchers. *Qualitative Report*, *24*(13), 44–57. https://doi.org/10.46743/2160-3715/2019.4120

Lacey, A., & Luff, D. (2009). Qualitative Data Analysis. *National Institute for Health Research*, 13.

Laghari, A. A., He, H., Khan, A., Kumar, N., & Kharel, R. (2018). Quality of experience framework for cloud computing (QoC). *IEEE Access*, *6*(December 2017), 64876–64890. https://doi.org/10.1109/ACCESS.2018.2865967

Levinson, M. (2007). *Software as a Service (SaaS) Definition and Solutions*. https://www.cio.com/article/272086/web-services-software-as-a-service-saas-definition-and-solutions.html

Maxwell, J. (George M. U. (1941). *Qualitative Research Design: An Interactive Approach* (3rd ed.). https://eclass.uop.gr/modules/document/file.php/1740/υλικό για διάβασμα/Qualitative

Research Design An Interactive Approach by Joseph A. Maxwell %28z-lib.org%29.pdf?utm_source=chatgpt.com

Miles, M. B., & Huberman, A. M. (1994). *Qualitative Data Analysis* (2nd ed., Vol. 1304). https://vivauniversity.wordpress.com/wp-content/uploads/2013/11/milesandhuberman1994.pdf

Mohd Ishak, N., & Abu Bakar, A. Y. (2014). Developing Sampling Frame for Case Study: Challenges and Conditions. *World Journal of Education*, *4*(3), 29–35. https://doi.org/10.5430/wje.v4n3p29

Nedelcu, B., & Stefanet, M.-E. (2019). Cloud Computing and its Challenges and Benefits in the Bank System. *Database Systems Journal*, *VI*(1), 44–58.

Riad Jaradat, M.-I., Ababneh, H., Al Fagih, K., Riad Mousa Jaradat, M.-I., Ababneh, H. T., S Faqih, K. M., & Nusairat, N. M. (2020). Exploring Cloud Computing Adoption in Higher Educational Environment: An Extension of the UTAUT Model with Trust. *International Journal of Advanced Science and Technology*, *29*(5), 8282–8306. https://www.researchgate.net/publication/341775850

Sajid, M., & Raza, Z. (2013). Cloud Computing: Issues & Challenges. *International Conference on Cloud, Big Data and Trust*, 13–15. https://scholar.googleusercontent.com/scholar?q=cache:aR5j3shKGh0J:scholar.google.com/+disadvantages+of+cloud+computing&hl=en&as_sdt=0,5

Smusin, M. (2023). *Cloud Computing in Banking: Benefits, Challenges and Best Practices*. https://yellow.systems/blog/cloud-computing-in-banking

Solomon, K. (2017). *Hybrid Cloud Computing and Service Environment for Ethiopian Banks A Thesis Submitted in Partial Fulfillment of the Requirement for the Degree of*.

Sriram, S. (2011). Cloud Computing in Banking: What banks need to know when considering a move to cloud. *Capgemini Consulting Technology Outsourcing*, 12. https://www.capgemini.com/wp-content/uploads/2017/07/Cloud_Computing_in_Banking.pdf

Taherdoost, H. (2022). What are Different Research Approaches? Comprehensive Review of Qualitative, Quantitative, and Mixed Method Research, Their Applications, Types, and Limitations. *Journal of Management Science & Engineering Research*, *5*(1), 53–63. https://doi.org/10.30564/jmser.v5i1.4538

Venkatesh, V., & Davis, F. D. (2000). Theoretical extension of the Technology Acceptance Model: Four longitudinal field studies. *Management Science*, *46*(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

Zergaw, C. (2023). *Zergaw Cloud*. https://zergaw.com/

Appendix I

Interview Guide for Banks

1. Can you describe your current IT infrastructure and how it supports your bank's operations?
2. What are your perceptions regarding the impact of local cloud services on security and data protection?
3. How do you view the potential benefits and challenges of local cloud services for regulatory compliance?
4. What concerns do you have about managing data sovereignty and residency with local cloud services?
5. How do you perceive the potential benefits and challenges of improvements in service availability and reliability with local cloud adoption?
6. What are your thoughts on the potential benefits and challenges of local cloud services to help address cyber-crimes?
7. How do you view the flexibility that local cloud services could offer to the banking operations?
8. How might local cloud adoption influence your bank's cost management strategies?
9. What are your thoughts on the benefits and challenges of local cloud services for data recovery processes?
10. What specific concerns or barriers do you have regarding the adoption of local cloud services?
11. How do you perceive the difficulties in integrating local cloud services with your legacy systems?
12. What are your concerns about vendor lock-in with local cloud services?
13. What misunderstandings regarding responsibilities with local cloud service providers are you aware of?
14. What security protocols would you expect from a cloud provider to meet your bank’s security needs?
15. What role do you see cloud computing playing in the future of banking in Ethiopia?
16. What innovations or advancements do you hope to see from local cloud providers to better support the banking sector?
17. In your opinion, what could accelerate the adoption of cloud services in the banking industry?

Appendix II

Interview Guide for Cloud Service Providers

1. Can you provide an overview of the cloud services your company offers to banks in Ethiopia?
2. How does your cloud service enhance security and data protection for banks and what possible challenges do you face?
3. How would you help banks with regulatory compliance to use your cloud services?
4. How does your service address data sovereignty and residency requirements for banks?
5. What measures do you take to ensure service availability and reliability for your clients?
6. How does your services help banks combat cyber-crimes and what challenges do you face in helping banks combat cyber-crimes?
7. How do your cloud services provide flexibility to banking operations?
8. How do you address concerns related to vendor lock-in for your clients?
9. What cost benefits does your cloud services offer to banks?
10. How do you support banks in data recovery processes and how do you address data recovery challenges?
11. How do you handle integration issues with banks' legacy systems?
12. What are the common misunderstandings regarding responsibilities between you and your banking clients?

Appendix III

Interview Guide for NBE.

1. What are the NBE's regulations and guidelines regarding data residency for banks considering cloud adoption, and how does the NBE ensure that banking data stored in cloud environments remains within Ethiopian jurisdiction?
2. How does the NBE address cybersecurity concerns in cloud adoption by banks, and what measures are in place to protect sensitive banking data from cyber threats?
3. What data protection requirements has the NBE established for banks planning to adopt cloud services, particularly regarding privacy, risk management, and the safeguarding of customer data?
4. What are the NBE's expectations regarding the auditing and compliance processes for banks using cloud services, particularly in relation to data security and regulatory standards?
5. What specific compliance requirements has the NBE established for banks that wants adopt cloud services, particularly in areas of data security, privacy, and risk management?
6. How does the NBE evaluate and approve cloud service providers to ensure they meet the regulatory standards required for handling banking data?
7. How does the NBE monitor banks' compliance with regulatory requirements when they utilize cloud services?
8. What are the potential penalties or corrective actions imposed by the NBE if a bank fails to comply with cloud-related regulations?
9. What are the NBE's expectations regarding risk management practices for banks if they start using cloud services, particularly in terms of data protection and disaster recovery?
10. How does the NBE ensure that auditing processes are robust and effective for banks if they start operating in a cloud environment?

Appendix IV

Interview Guide for INSA.

1. What specific security standards does INSA recommend for local cloud service providers hosting sensitive banking data?
2. Does INSA have any guidelines on how banks should assess the security capabilities of local cloud service providers?
3. What measures should local cloud providers implement to protect banks from emerging cyber threats such as ransomware, phishing, and insider attacks?
4. What are the main compliance challenges INSA foresees for banks adopting local cloud services, and how can these be addressed?
5. Does INSA provide certifications or audits for local cloud providers to ensure they meet national security and compliance standards?
6. What role does INSA play in preventing and responding to cybercrimes targeting cloud-based banking services?
7. What are INSA's expectations for local cloud providers regarding disaster recovery, incident response, and regular testing of these capabilities?
8. What innovations or advancements would INSA like to see from local cloud providers to better support the security and operational needs of Ethiopian banks?
9. What steps or initiatives does INSA believe could accelerate the secure adoption of local cloud services by the banking sector in Ethiopia?
10. What penalties or consequences are in place for cloud service providers or banks that fail to meet security or compliance requirements?