
# Addis Ababa University

# School of Commerce Graduate program

## Business Information System (BIS)

## Comparison of hybrid, cloud, and on-premise deployment of AD: In the case of Ethiopian Banks

**Advisor: Eyob Nigussie (PhD)**

**Prepared by: Hanna Mekonen**

**Date June, 2024**

# Comparison of hybrid, cloud, and on-premise deployment of Active Directory: In the case of Ethiopian Banks

**Hanna Mekonen**

**A Thesis Submitted to**

**The Department of Business Information System (BIS)**

**Presented in Partial Fulfillment of the Requirement for the degree Master of Business Information System**

**Addis Ababa University**

**Addis Ababa, Ethiopia**

June, 2024

# Addis Ababa University

# School of Commerce Graduate program

## DECLARATION

This is to certify that the thesis prepared by Hanna Mekonen, entitled: "Comparison of hybrid, cloud, and on-premise deployment of Active Directory: In the case of Ethiopian Banks". My advisor, Eyob Nigussie (PhD) oversees the study. This thesis has not been previously presented for academic purposes at the university level. All sources used in the research have been properly cited.

Signed by Examining Committee:

External Examiner: Dr. Tibebe Signature _____ Date _____

Internal Examiner: Dr. Hailay Beyene Signature _____Date _____

Advisory: Dr. Eyob Nigussie Signature _____Date _____

**By: Hanna Mekonen**

# ACKNOWLEDGEMENT

I thank Almighty God for blessings, insight, courage, strength, and opportunities in my life. I am grateful to my research advisor, Dr. Eyob Nigussie for facilitating my study and providing valuable guidance throughout the process. I am grateful to the Different Bank's employees who participated in the interview and expert validation sessions. Your essential efforts made this study possible. Finally, I would like to express my gratitude to all lecturers and administrative personnel at the School of Business Information Science for their steadfast support and advise throughout my studies.

# List of figures

# List of Acronyms and Abbreviation

1. AD ----------Active Directory
2. CBE ----------Commercial Bank of Ethiopia
3. BIS----------Business Information System
4. BoA ----------Bank of Abyssinia
5. DB ----------Dashen Bank
6. AB ----------Awash Bank
7. AWS ----------Amazon Web Service
8. HR ----------Human Resource
9. IT----------Information Technology
10. IS---------- Information System
11. BW----------Band Widths
12. CC----------Cloud Computing
13. NaaS----------Network as a Service
14. SaaS----------Software as a Service
15. IaaS----------Infrastructure as a Service
16. IBM----------International Business Machine
17. ABAC----------Attribute-Based Access Control
18. CSP----------Cloud Service Provider
19. GCP----------Google Cloud Platform
20. ADDS----------Active Directory Domain Services
21. GPOs----------Group Policy Objects
22. OU----------Organizational Unit
23. ACL----------Access Control Lists
24. SSO----------Single Sign-On

25. CapEx----------Capital Expenditures

26. PCI DSS----------Payment Card Industry Data Security Standard

27. OS----------Operating System

28. TCO----------Total Cost of Ownership

29. AAD----------Azure Active Directory

30. ADFS----------Active Directory Federation Services

31. RBAC----------Role-Based Access Control

32. IGI ----------Identity Governance and Intelligence

33. IAM----------Identity and Access Management

34. FIM----------Federated Identity Management

35. LDAP----------Lightweight Directory Access Protocol

36. CRM----------Customer Relationship Management

37. SOA----------Service Oriented Architecture

38. EDA----------Event Driven Architecture

39. ETL----------Extract, Transform, and Load

40. CSA----------Cloud Security Alliance

41. ISO----------International Organization for Standardization

42. CSC----------Cloud Service Consumers

43. GDPR----------General Data Protection Regulation

# Abstract

This study examines current state of IT infrastructure in Ethiopian banks, by comparing on-premises, cloud and hybrid models of Active Directory deployment. The purpose of this research paper is to recommend best of Active Directory deployment options for Ethiopian banks by referring pros and cons of on-premises, hybrid, and cloud Active Directory deployment options for Ethiopian banks.

The strategic considerations, operational obstacles, and practical ramifications of each deployment strategy collected in-depth interviews with IT professionals from major Ethiopian banks, as well as extensive case studies of their IT infrastructures. Motivations driving deployment decisions, operational and staffing ramifications, tactics for ensuring consistency in identity and access management, and broader implications for IT governance and security are among the topics covered.

The findings indicate that different needs and objectives influence deployment decisions, with some institutions emphasizing the flexibility and scalability provided by cloud deployment, while others value the control and security of on-premise systems. Hybrid deployment develops as a compromise, reflecting the nuanced techniques need to meet bank-specific difficulties. A one-size-fits-all approach is unlikely to succeed because each bank has distinct needs and current infrastructure. Ethiopian banks can create a personalized cloud strategy by carefully examining their current IT landscape and future ambitions.

The discussion focuses on the implications for the broader banking sector, drawing parallels to international best practices and recommending areas for future research and practical implementation. A hybrid cloud architecture that blends on-premises infrastructure with public and private cloud environments may be the best option for many Ethiopian banks. This strategy enables banks to maintain control over sensitive data while taking advantage of cloud computing's scalability and cost-efficiency. Banks must address security and compliance concerns with strong measures such as application-level encryption and privileged access.



**Keywords:** Active Directory, On-Premises, Cloud Computing, Hybrid Cloud Computing.

Contents

# Chapter One

## Introduction

Active Directory (AD) is Microsoft's proprietary directory service. It runs on Windows Server and enables Active Directory administrators to manage permissions and access to network resources. Active Directory stores data as an object. An object is a single element, such as a user, group, application or device such as a printer and scanner. Objects are normally defined as either resource, such as printers or computers, or security principals, such as users or groups (Gillis, 2023).

On-premises Active Directory deployment is process of setting up and operating an Active Directory infrastructure within an organization's internal network. This includes the creation and maintenance of a centralized directory service for user and device authentication, as well as the delivery of services such as group policy management, user and device provisioning, and security audits (Cybellium, 2023).

Cloud computing, is the use of distant servers and internet-based applications. Cloud-based Active Directory service used to handle user identities, authentication, and access control in the cloud is referred to as cloud deployment of Active Directory (Assefa, 2018).

A hybrid deployment of Active Directory refers to a configuration that permits on-premises Active Directory and cloud-based Active Directory (such as Azure Active Directory) to coexist. This setup allows for the smooth integration and management of user identities, authentication, and access control between on-premises and cloud systems (Giuseppe Di Federico, 2022).

The Bank industry's high security and compliance requirements, the deployment of Active Directory in a hybrid and cloud setting vs on-premises deployment provides distinct issues for banks.

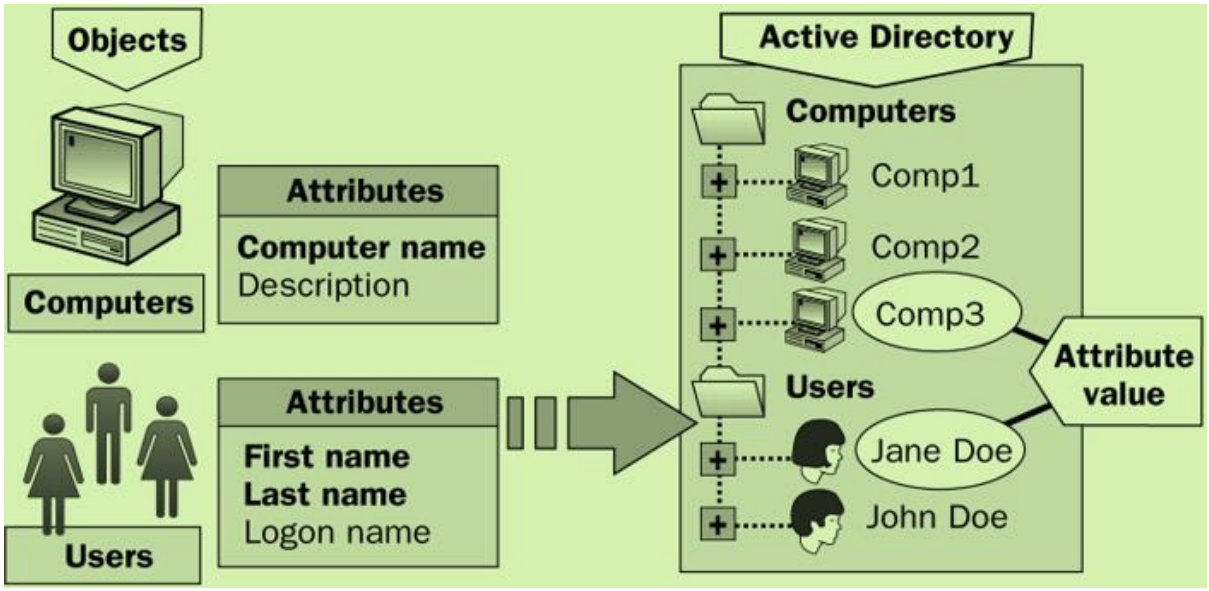



Figure 1. Active Directory object and attribute

### 1.1 Background of the Study

The Ethiopian Banking Landscape The financial sector is expanding, and IT infrastructure is becoming increasingly important. User access management has always been based on on-premises Active Directory. Rising security concerns, regulatory regulations, and the need for greater operational efficiency. Some banks have a limited number of technological skills and resources. Internet access is unevenly spread and occasionally inconsistent throughout the country.

Global Trends for Active Directory Deployment of Scalability, cost-effectiveness, and flexibility may all be improved by shifting to hybrid and cloud installations. Increased emphasis on security and compliance in response to cyber threats and legislation. New cloud technologies and managed services are emerging to improve Active Directory management efficiency (Giuseppe Di Federico, 2022).

Active Directory synchronization is the process of merging an on-premises Active Directory with a cloud-based instance of Active Directory. To enable Active Directory synchronization each deployment, organizations can use solutions

### 1.2 Statement of the Problem

Active Directory stores login information for accounts and information about other networked resources. It organizes information in a hierarchical manner. AD is dynamic, as opposed to a basic database, which is only a storage tool; it allows administrators to search and manage the

database's resources, ensuring that the network hierarchy is appropriately structured at all times ((Binduf, 2018, April).

This study attempts to close this gap by conducting a comparative analysis of hybrid, cloud, and on-premise AD deployment options in Ethiopian banks.

Cost Efficiency: The comparative cost implications of hybrid, cloud, and on-premise AD deployments,

The analysis will evaluate each model based on essential criteria for the banking sector, including effectiveness and performance, including hybrid, cloud-based, and on-premise AD implementations compare in terms of stability, scalability, and overall system effectiveness in Ethiopian banks.

Security and Compliance: The security implications and regulatory compliance considerations connected with each deployment strategy, and how they relate to Ethiopian banking's specific regulatory environment.

## 1.3 Research Question

RQ1: What are the initial setup costs and continuing operating expenditures associated with hybrid, cloud, and on-premise AD implementations throughout their lifetime in Ethiopian banks and how do cost concerns differ among deployment options, including license fees, infrastructure maintenance, and scaling costs?

RQ2: What are the security implications of hybrid, cloud, and on-premise AD implementations for Ethiopian banks, especially in terms of data protection, access restrictions, and regulatory compliance and how do these deployment strategies satisfy the unique regulatory constraints and data sovereignty considerations that the Ethiopian banking industry faces?

RQ 3: What are the operational efficiency and performance metrics? How do hybrid, cloud-based, and on-premise deployment methods of Active Directory (AD) systems fare in terms of scalability and dependability in Ethiopian banks?

## 1.4 Research Objective

### 1.4.1 General Objective

To provide insights for effective Active Directory deployment and management strategies by identifying benefits, and challenges of each Active Directory deployment.

### 1.4.2 Specific Objective

Analyse the initial expenses of each deployment and budgets for hardware, software license, maintenance, and expertise in Ethiopian banks.

To assess each deployment model's performance with respect to authentication times, user access, and system responsiveness.

Compare the security aspects of each deployment type considering data privacy legislation and cyber security concerns.

Compare the Active Directory administrative complexity and IT skill required to manage Active Directory across deployment models.

## 1.5 Significance of the study

Banks all over the world are realizing how important it is to choose among available deployment environment including the public or private cloud and utilizing hybrid and multi-cloud strategies in order to guarantee customer pleasure, data security, and regulatory compliance. Active Directory additionally, since a cloud computing framework is modern context, it designed specifically for the Ethiopian banking sector has been put forth, stressing the value of combining private and public clouds and underscoring the importance of researching the various Active Directory deployment options.

## 1.6 Scope of the Study

The main focus of the proposed thesis is on Ethiopian banks' growing use of hybrid cloud technologies, which blends public and private clouds. As a result, the study is pertinent given the rapidly changing technical environment and the particular comparison of cloud computing frameworks and On-premises that Ethiopia's banking sector is currently considering.

## 1.7 Limitation of the study

**Limited sample size:** Currently only few banks are used Active Directory for resource management, this might reduce the generalization of the findings.

**Lack of long-term data:** Most Ethiopian Banks are used the modern centralized system in recent time.

**On self-reported data:** interviews with bank IT workers will be one of data collection technique used in this study, so the results may be subjective and prone to bias or mistakes.

**Cost analysis:** Each deployment strategy, particularly in terms of long-term maintenance and scalability couldn’t get real numerical and financial data.

**Ethiopian context consideration:** Ethiopian banks still suffer networking issue like internet bandwidth and banking regulation related with data sovereignty and data privacy rules reviews suddenly and fully applicable.

**Neglecting Updated Technologies:** rapid growth of cloud technology and security solutions doesn't give the opportunity to upgrade regularly in Ethiopian banks.

### 1.8 Definition of Terms

**Digital Transformation:** Adopting digital technology by an organization's existing all IT infrastructure and technology utilization to better fulfill customer expectations.

**Active Directory:** is a Database and set of service runs in windows operating system used to centrally managing networked resources.

**On-Premises Deployment:** installation of software, hardware, and other IT objects within an organization's own data center.

**Cloud Deployment:** cloud computing, is the use of distant servers and internet-based applications to store, manage access data and resources.

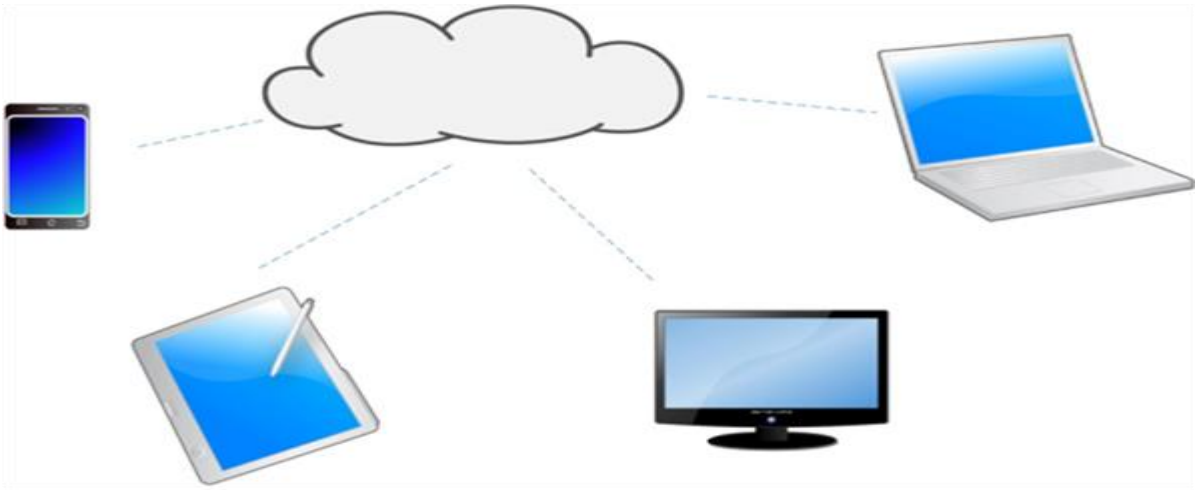


Figure 2. Cloud deployment

**Hybrid Deployment:** paradigm combines on-premises and cloud deployment methodologies.

**Hybrid cloud:** cloud computing system that mixes on-premises infrastructure with a public or private cloud.

**Deployment of Active Directory on Private Cloud:** It refers to the installation and maintenance of an Active Directory server within the organization's on-premises architecture

and user controls the private cloud, and it owns the hardware, software, and other supporting infrastructure.

**Active Directory Deployment in Public Cloud:** entails utilizing Active Directory services supplied by a third-party cloud service provider (CSP) such as Amazon Web Services (AWS), Google Cloud Platform (GCP), or Azure.

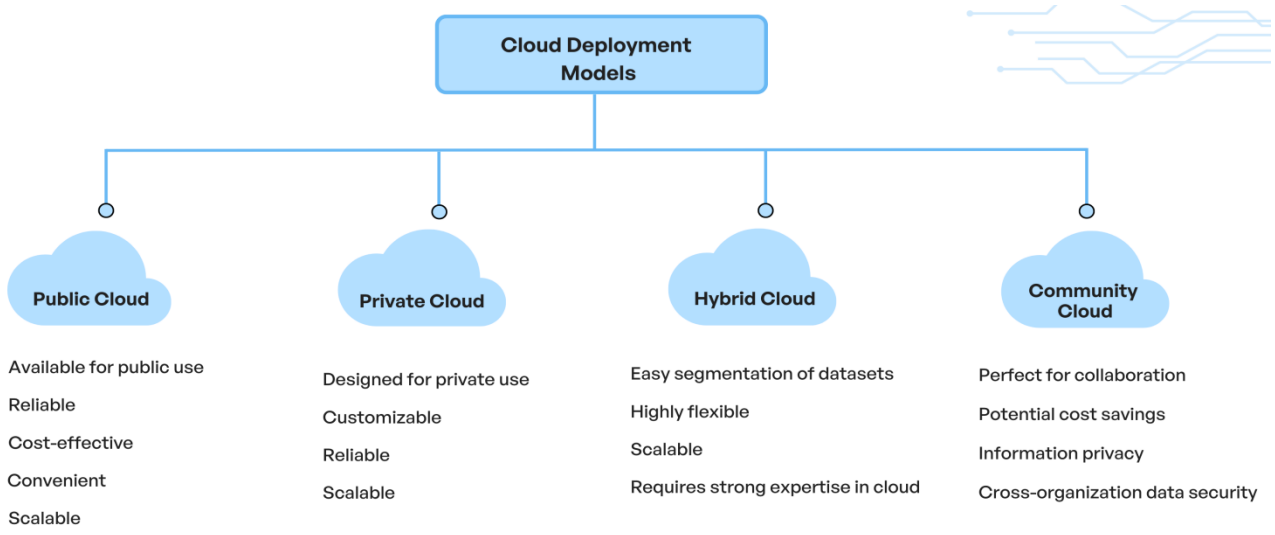



Figure 3. Types of cloud deployment model

## 1.9 Organization of the research

The research is organized in five chapter:

Chapter 1: Contains introduction, Background, Statement of the problem, Objective of the study, Significance of the study, Scope and limitations

Chapter 2: It introduce review of related literature and continue to overview of Business information system, Banking business industry and information system, Empirical studies of Comparison of hybrid, cloud, and on-premise, Empirical studies of Comparison of hybrid, cloud, and on-premise deployment of Active Directory, Types of Active Directory Deployment, Selection of hybrid, cloud, and on-premise deployment of Active Directory, Related work in Ethiopian bank

Chapter 3: Contain Research Methodology, Research Design, Data Type and Source, Research strategy, Sampling procedure, Strategies for data collection, Data collection method and tools, Data presentation.

Chapter 4: presents the overall finding of the study which prevails about the most important and frequently occurring causes of delay

Chapter 5: encompasses the conclusion and recommendation part of the study. Conclusions are be made from the previous chapter so that we can make some recommendations.

# CHAPTER TWO

## Review of Related Literature

### 2.1 Introduction

In chapter two, the review of related literature is presented, covering various topics related to Comparison of hybrid, cloud, and on-premise deployment of Active Directory. The variations in deployment approaches for Active Directory systems can provide light on the ramifications of using hybrid, cloud, or on-premise deployment strategies. Researchers may investigate how each model affects elements such as cost-effectiveness, data management, scalability, and security, providing a thorough grasp of the factors to consider when deciding on the best deployment technique for Application Delivery systems.

### 2.2 Overview of Business Information System

A business information system (BIS) is a formal socio-technical and organizational system that collects, processes, stores, and distributes data. It is a critical component of modern corporate operations, allowing firms to conduct their activities more efficiently and successfully. BIS incorporates a variety of components, including hardware, software, databases, networks, and procedures, to ease information flow and decision-making processes. A business information system is an important part of modern company operations since it integrates diverse components to enable the effective administration of organizational activities. Its principal goal is to offer timely and reliable information to assist decision-making processes and strategic planning, resulting in improved overall organizational performance (Beynon-Davies, 2019).

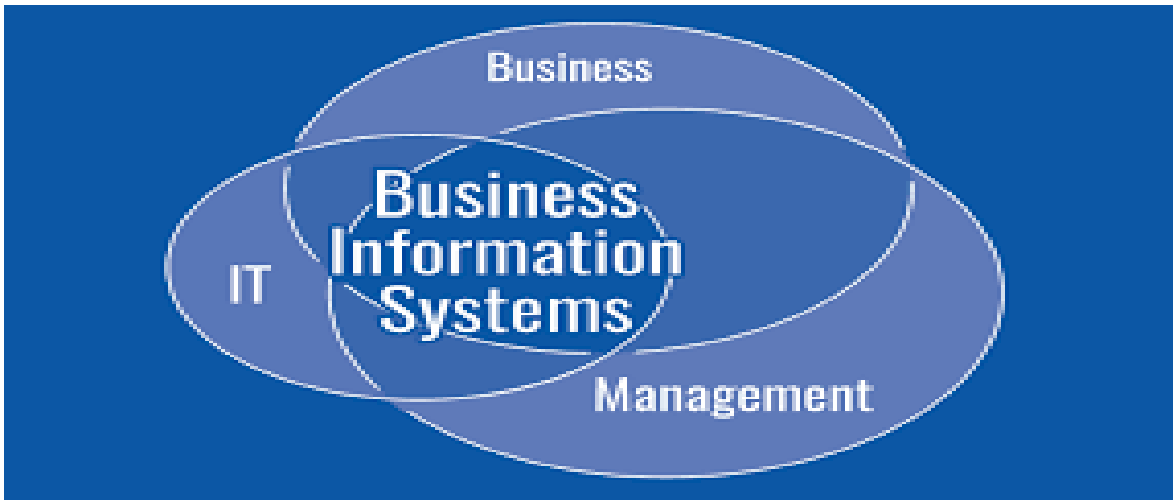



Figure 4. Business Information System

### 2.3 Banking business industry and Information System

The banking business relies significantly on information technologies to run its operations efficiently. Banks acquire, process, and store massive volumes of data on consumer accounts, transactions, and financial records. In the banking business, IS are utilized for several reasons, such as:

Client account management: IS keeps track of client information, account balances, and transaction histories.

Loan processing and underwriting: IS automates loan applications, evaluates creditworthiness, and originates loans. Fraud detection and prevention: IS keeps an eye out for unusual activities and helps to prevent fraud (Ahmad, 2019).

Regulatory compliance: IS enables banks to comply with complicated financial rules.

Risk management: IS gives banks the information they need to analyze and manage risk.

Product creation and innovation: IS allows banks to create and market new goods and services.

Customer service: IS offers online and mobile banking, as well as call centers and other customer care options.

However, implementing information technology in banks necessitates considerable expenditures, stringent security measures, and the duty of avoiding data loss. Banks must ensure that their information systems are safe, dependable, and meet regulatory criteria. The banking business relies significantly on information technologies to run operations, make decisions, and provide services to clients. The proper use of information technology is vital for the development and survival of banks in today's competitive environment (Ali, 2022).

## 2.4 Active Directory

**Active Directory** (AD) is a directory service to manage and organize resources in a networked environment. It offers centralized authentication, authorization, and directory services to users, computers, and other network devices. Here's a summary of its main components and features:

**Domain Services:** Active Directory Domain Services (AD DS) is Active Directory's basic component. It organizes information about people, groups, machines, and other network objects into a hierarchical structure called a domain. Domains can be linked together to construct domain trees and domain forests, which allow for centralized control across numerous locations or organizational units.

**Authentication and Authorization:** AD offers authentication services, letting users to access the network using their credentials (username and password). It also provides authorization by building access control lists (ACLs) that determine user rights on network resources. This guarantees that users can only access the resources that they are permitted to utilize.

**Directory Services:** AD is a directory service that stores and organizes information about network resources in a systematic manner. This comprises information about user accounts, group memberships, machine setups, and other network administration-related properties. Directory data is duplicated among domain controllers in the network to ensure fault tolerance and availability.

**Group Policy:** Active Directory. Group Policy enables administrators to design and enforce security policies, configuration settings, and software deployment rules across the whole network. Group Policy Objects (GPOs) can be used at the domain, site, or organizational unit (OU) level to manage user settings, system configurations, and security settings ((Binduf, 2018, April).

**Trust Relationships:** Active Directory enables trust relationships across domains, forests, and external directories, allowing for smooth access to resources across administrative borders. Trust relationships may be formed to allow users from one domain to access resources in another domain or forest while preserving security limits and access rules.

AD employs a multi-master replication strategy to synchronize directory data among domain controllers in the network. This guarantees that any changes made to directory objects are effectively and uniformly propagated across all domain controllers. Fault tolerance measures like as redundancy, backup, and disaster recovery are used to assure data availability and integrity (McDonald, 2022).

Active Directory interfaces with a variety of Microsoft services and applications, including Exchange Server (email), SharePoint (collaboration), and Office 365 (cloud-based productivity tools). This connection allows single sign-on (SSO), unified identity management, and seamless mise and cloud services.

Overall, Active Directory is vital for organizing, managing, and safeguarding resources in a networked environment, making it an essential component of contemporary IT infrastructure for businesses of any size.

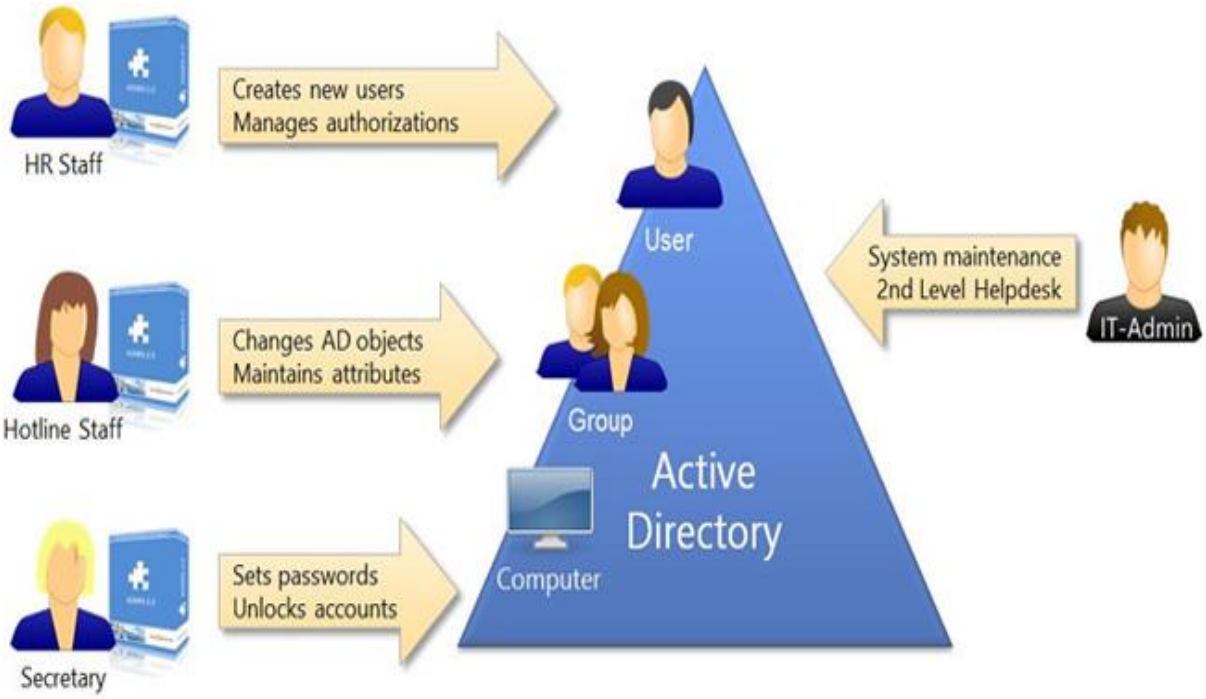



Figure 5. Active Directory

### 2.4.1 Empirical studies of Comparison of each deployment of Active Directory

Although there aren't many extensively disseminated empirical studies that compare Active Directory deployment options—hybrid, cloud, and on-premise—you may still use research and information to guide your selection. Here's how to go about it:

**1. Industry Reports and Analyst Opinions:** Look for industry reports on cloud usage for Active Directory from Forrester, Gartner, or IDC. Cost comparisons and deployment trends data are frequently included in these reports.

**2. Case Studies:** Seek out case studies that demonstrate effective Active Directory deployments in cloud or hybrid environments from Microsoft or other suppliers. These can offer practical insights regarding difficulties and performance.

**3. Emphasis on Specific Evaluation Criteria:** Determine the important considerations for your choice (security, affordability, scalability, etc.) and conduct separate research on each one rather to relying on a single comprehensive study (Subbarao, 2023)

**Security:** Here is a general road map that covers some of the key features and services for establishing a stronger security posture following Active Directory deployment.

**Cost:** When comparing on-premise hardware and software licensing to continuous subscription rates for cloud-based Active Directory, take into account the one-time expenditures.

**Scalability:** As your demands expand, cloud deployments make it simpler to scale resources.

The ideal deployment model is determined by your unique requirements and available resources. Choosing between hybrid, cloud, or on-premise Active Directory requires careful consideration of various aspects, including your budget, existing infrastructure, IT experience, and security requirements (Zannone, 2023)

### 2.4.2 Types of Active Directory Deployment

There are various approaches to deploy Active Directory, each having pros and downsides of their own. The primary forms of Active Directory deployments are as follow:

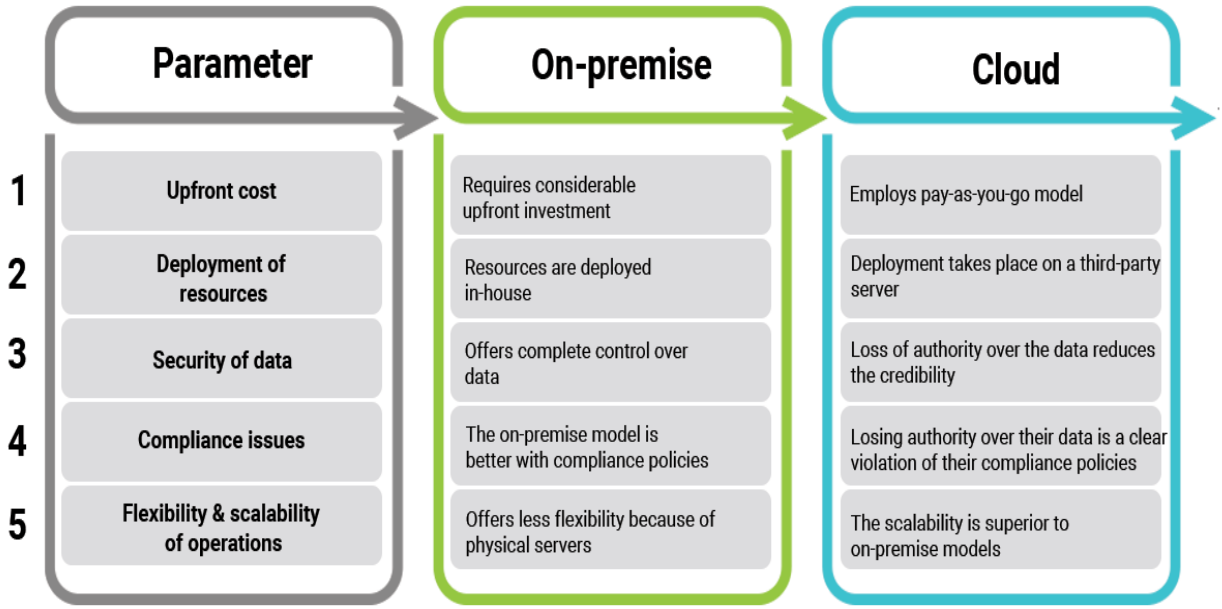



Figure 6. List of key differences between Cloud and On-premise

**1. On-Premise Deployment:** This option eliminates various tasks associated with on-site data centers and improves control and data privacy. It is preferred for companies with security concerns and the need for customized solutions. Offers better control and data privacy as the infrastructure and systems are accessible at all times.

**2. Deployment of Cloud Infrastructure:** provides decreased latency, agility, and cost savings. Enables companies to scale their resources as necessary and eliminates the need to purchase IT resources by offering effective infrastructure and services. Lowers the cost of purchasing, implementing, and maintaining software and hardware as well as eliminates capital expenditures (CapEx) due to virtualization of capital assets.

**3. Hybrid Cloud Implementation:** balances control and flexibility by utilizing the public cloud's scale to enable the on-premises storage of sensitive data.

Allows workloads to be phased in gradually over time, enabling a gradual transfer to the cloud. Accurate implementation requires reliable servers, storage, and network capabilities (Francis D. .., 2017).

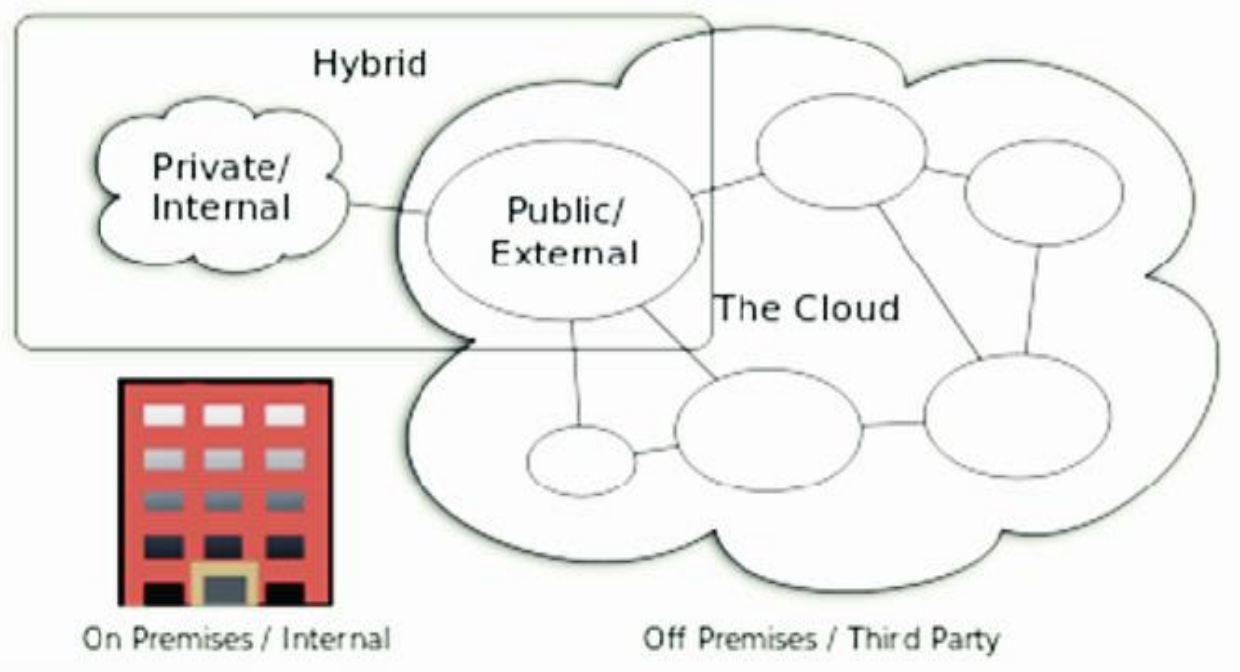



Figure 7. Hybrid-cloud Deployment-model-example

## 2.5 Selection of hybrid, cloud, and on-premise deployment of Active Directory

Active Directory (Active Directory) can be deployed in a variety of ways, each with their own set of benefits and disadvantages. The following are the main types of Active Directory deployments:

1. **On-Premise** The standard deployment model for Active Directory (AD DS) involves running it on your own physical servers.

Advantages: Gives you complete control over your data and security, which is ideal for enterprises with stringent compliance needs.

Disadvantages: Management requires significant IT experience and resources, can be expensive owing to hardware and software costs, and has restricted scalability (Francis D. , 2021).

2. **Cloud Active Directory (Cloud AD):**

Microsoft provides a cloud-based identity and access management service.

Advantages: Scalability, no need for on-premise servers, and simplified management.

Disadvantages: For integration, existing applications may need to be changed.

3. **Hybrid Deployment:** Combining on-premises and Azure Active Directory to provide a single identity management solution.

Advantages: Provides the flexibility to exploit both on-premise and cloud benefits, which is beneficial for enterprises who are progressively shifting to the cloud.

Disadvantages: More difficult to maintain than a single deployment approach; necessitates meticulous planning and configuration.

The optimum deployment choice for you is determined by your individual requirements and preferences. Consider your existing infrastructure, security requirements, money, and IT skills when making your decision (Banstola, 2021).

### 2.4.3 The Main Security Difference

Active Directory on-site: Complete control over the infrastructure is made possible by on-premise Active Directory, which enables businesses to physically safeguard their computers and set up the network to suit their requirements.

Data Residency: Sensitive information is kept on the organization's property, guaranteeing that it is not kept outside of its authority. This is crucial for sectors with stringent data rules.

Security Guidelines: Strict security regulations may be implemented using on-premise Active Directory and customized to meet the unique requirements of the company.

Active Directory in the Cloud: Security Updates: To keep Azure Active Directory secure, cloud service providers such as Microsoft make sure that the most recent security patches are implemented on a regular basis.

Cloud-based solutions can grow quickly to meet demand, lowering the risk of security breaches caused by infrastructure overload.

Conditional Access: Azure AD provides sophisticated security capabilities including as conditional access, identity protection, and security reporting that improve the overall security posture.

Hybrid Active Directory: Security: Hybrid approaches combine the benefits of on-premise and cloud-based solutions, striking a balance between control and scalability. However, security in hybrid systems may be difficult and requires careful management to guarantee that both on-premise and cloud components are appropriately secured (Raza, 2019).

Key Differences: Data Ownership: In on-premise Active Directory, the organization keeps complete ownership and management of data, but in cloud-based solutions, data is kept on the provider's servers, raising questions about data residency and compliance.

Security Responsibility: In cloud-based systems, there is a shared responsibility model wherein the provider manages certain aspects of security, while in on-premise Active Directory, the business bears full responsibility for security (Sangwan, June 2015).

In conclusion, cloud-based Active Directory offers increased security capabilities and scalability, but comes with a shared responsibility model and potential data residency concerns. On-premise Active Directory, on the other hand, gives better control over data and security regulations. Although hybrid Active Directory provides scalability and control in equal measure, it needs to be managed carefully to guarantee adequate security.

### 2.4.4 Scalability in compared each deployment

Scalability of On-Premises Active Directory: The capacity of the infrastructure has a major impact on how scalable on-premises Active Directory may be. Scaling frequently necessitates complicated setups and the replication of domain controllers. IT staff are burdened further since they have to plan for expansion and buy gear appropriately.

Scalability of Cloud-Based Active Directory: As a cloud-based solution, Azure Active Directory has built-in scalability. Users just pay for the amount they use, and it can grow immediately to match demand. Because Microsoft handles maintenance activities like patching and upgrades, users have less administrative work to do.

Scalability of Hybrid Active Directory: The on-premises and cloud components of hybrid Active Directory are combined, and each enhances total scalability:

The on-premises component is restricted by the capacity of the local infrastructure, which may be improved or increased as needed.

Cloud Component: The cloud component, which is often AAD, allows for scalability and flexibility of cloud resources and applications.

Integration and Synchronization: The on-premises and cloud components are integrated and synchronized to guarantee that user identities and access remain consistent across both environments.

However, hybrid systems may need additional planning and infrastructure changes to attain the same degree of immediate scalability as cloud-based solutions. In essence, cloud-based AD systems, such as Azure AD, have the most inherent scalability due to their cloud-native nature. Hybrid AD offers a blend of local control and cloud-based scalability, whereas on-premises AD has the most constrained scalability, relying mainly on local infrastructure capabilities.

### 2.4.5 Cost implication of deployment option

Active Directory on-site

Servers: Dedicated servers are needed for on-premise Active Directory, and they can be costly, particularly if a server room needs to be maintained. Server's cost anything between $1,000 and $30,000 per.

Software: Windows Server licenses, which are priced according to CPU core count, must be purchased. Increased expenses for many servers may result from this.

Licensing: Depending on the number of users or devices, client access licenses (CALs) are necessary, which raises the total cost.

Upkeep: Updates, patches, and troubleshooting are just a few of the administrative tasks necessary to maintain Active Directory on-premise. This may be expensive and time-consuming.

Cloud AD: (Azure Active Directory)

Azure Active Directory (AAD) is a cloud-based solution, which eliminates the need to invest in hardware or maintain a server room. This minimizes the upfront price of servers and lowers recurring maintenance charges.

Azure AD Premium license provides a cost-effective alternative to on-premise systems, particularly for smaller enterprises.

Azure AD offers excellent scalability, enabling for easy addition and removal of users and resources without requiring hardware changes.

Azure AD has strong security features including conditional access, identity protection, and security reporting, which can decrease the need for additional security tools and expertise (Trovato, 2019).

**Comparison**

Initial costs: On-premise Active Directory involves large upfront expenditures in infrastructure and software. whereas these expenses are eliminated by Azure Active Directory.

Ongoing Costs: Azure Active Directory lowers these expenses through cloud-based management and scalability, whereas On-premise Active Directory necessitates continual administrative work and maintenance (Deb, 2021).

To summarize, when compared to on-premise Active Directory, Azure Active Directory provides a more affordable and expandable solution. Even though Azure AD comes with certain extra expenditures, such add-ons and licensing, these are frequently outweighed by the fact that less hardware and upkeep are required.

### 2.5 Related work in Banking Sector

**Banking Hybrid and Multi-Cloud Approaches**: According to a Retail Banker International article, banks throughout the world are seeking digital transformation through cloud Active adoption. The essay emphasizes the need of properly developing a cloud adoption strategy, and hybrid and multi-cloud models provide feasible routes forward, allowing banks to get the most out of their cloud investments while complying with regulatory obligations (Rashid, 2022).

**Hybrid Active Directory Environment Challenges and Solutions:** One Identity's white paper covers the difficulties of administering a hybrid Active Directory infrastructure and the significance of utilizing a single solution to handle the complete hybrid environment. It emphasizes the importance of avoiding typical implementation blunders and ensuring proper synchronization between on-premises Active Directory and Azure Active Directory (Banstola, 2021).

**Dashen Bank Active Adopts IBM Hybrid Cloud Solutions:** Dashen Bank in Ethiopia has used IBM Hybrid Cloud technologies to speed its digital transformation and fulfil the rising demand for digital-first customers. By implementing a hybrid cloud approach, the bank will be able to deploy and develop its digital channels across any technological environment, increasing its competitive edge and meeting changing consumer expectations (Dashen Bank partners, Aug 22, 2022).

**Adoption of Cloud Computing in Ethiopian Banks:** A study article on cloud computing adoption obstacles in example of Commercial Bank of Ethiopia examines security and privacy concerns, and availability of high-bandwidth connections, all of which are critical factors for banks when adopting cloud computing (Tesema, 2020)

| CLOUD | FEATURE | ON-PREMISES |
|---|---|---|
| Software is hosted and managed by a cloud provider. | Deployment | Software is installed and executed on the organization's servers. |
| Typically, pay-as-you-go subscription model. | Cost | Upfront capital expenditures for hardware and software, ongoing maintenance, and support costs. |
| It is easy to scale resources up or down as needed. | Scalability | More complicated and expensive to scale. |
| Applications and data can be accessed from anywhere with an internet connection. | Accessibility | Applications and data are only accessible from within the organization's network. |
| Cloud providers offer a wide range of security features and certifications. | Security | Security is the responsibility of the organization. |
| Cloud providers offer compliance solutions for a variety of industry regulations. | Compliance | The organization is responsible for ensuring compliance with all applicable regulations. |
| Cloud providers have a team of experts who manage and maintain the cloud infrastructure. | Expertise | The organization needs an IT team to manage and maintain its on-premises infrastructure. |

Figure 8. Cloud Vs On-Premises

# CHAPTER THREE

## Methodology

**Investigation and Analysis:** Analysed existing research and case studies on Active Directory adoption in the banking industry, focusing on emerging markets like Ethiopia.

Ethiopian Financial Scene: Conduct a detailed evaluation of Ethiopian banks' current IT infrastructure, data security regulations, and technological readiness.

Comparing deployment models: Compare and contrast the three deployment options: on-premises, hybrid, and cloud.

Initial investment: hardware/software procurement and maintenance are all costs.

Scalability and flexibility: refer to the capacity to react to changing user requirements and data quantities.

Data privacy, regulatory conformity, and disaster recovery capabilities are all examples of **security and compliance.**

System uptime, latency, and user experience are all examples of **performance and availability**.

**Benefits and hazards:** Examined the unique advantages and possible risks of each deployment option for Ethiopian banks.

### 3.1 Description of the Study Area

The research concentrated on the problems and potential associated with Active Directory implementation in hybrid and cloud settings as differ from on-premises deployment in the Ethiopian banking industry. The research is relying on current literature on Active Directory On-premises deployment, hybrid cloud, and cloud computing in the banking industry. The research had also taken into account the experiences of other banks in the area and throughout the world that have implemented goes from On-premises to hybrid and cloud models. (Assefa, 2018)

### 3.2 Research Approach

**Analysis of banking industry**: Analyzed Ethiopian banks' particular requirements and problems in terms of digital transformation, security, and compliance.

**Deployment of hybrid and multi-cloud infrastructur**e: Examined the growing trend of hybrid and multi-cloud installations in the banking industry, as institutions employ cloud-native and cloud-agnostic apps to guarantee seamless operations and future-proofing.

**Problems and solutions**: Identified the typical issues that banks experience when installing Active Directory in hybrid and cloud environments than On-premises and discuss potential solutions to these difficulties.

**Case studies include**: Examined particular instances of banks that have deployed On-premises as well as hybrid Active Directory installations effectively. Identified banks that have deployed AD using various deployment techniques and collecting pertinent information about their experiences.

### 3.3 Research Design

This study employs a qualitative case study technique to investigate and evaluate the various AD deployment models utilized by Ethiopian banks. A case study is an ideal way for providing a thorough grasp of a real-world occurrence in its natural environment. The case study is exploratory in nature, with the purpose of identifying critical features and obstacles specific to each AD deployment architecture.

Case Studies: A selective sample of Ethiopian banks is selected based on variables such as size, current IT infrastructure, and cloud usage. This enables for detailed comparisons between deployment models.

Semi-structured interviews were performed with key IT people at each bank, including IT managers, system administrators, and security specialists. Open-ended questions facilitated the discussion, allowing individuals to express their experiences and viewpoints.

Research Methodology: Understanding experiences, meanings, and viewpoints is the main goal of qualitative research. It makes in-depth investigation and analysis possible.
Research Type: To better understand and contrast the various AD deployment strategies used in Ethiopian banks, this study will be exploratory and descriptive in nature.

**Interview**

One of the main ways that qualitative research collects data is through interviews.

They make it possible for researchers to get comprehensive data straight from individuals.

It is possible to employ a variety of interview formats, including unstructured, semi-structured, and organized ones.

Depending on the goals of the study, interviews may be done in groups or one-on-one.

Planning, conducting, and analyzing interviews carefully is essential to the validity and dependability of the results of qualitative research.

**Case studies**

Case studies are comprehensive examinations of one or more instances over an extended period of time. The case can involve a specific person, program, activity, event, or time-and location-bound procedure. Case studies include a variety of data collecting techniques, including document analysis, observations, and interviews. They offer a comprehensive, contextual grasp of the topic being studied. Case studies can be descriptive, explanatory, or exploratory in character. Case study research requires careful case selection, data collecting, and analysis to ensure its validity and dependability.


Figure 9. Qualitative research methodology including interview and case study

### 3.4 Population and Sample

Access to Information: Contacted the IT departments or key stakeholders at the selected banks to inquire about their willingness to participate in the research and offer access to pertinent information regarding their AD deployments. Create clear communication channels and secure all required clearances for data collecting and sharing.

Create a framework for assessing various deployment options based on cost, scalability, flexibility, security, dependability, ease of administration, and alignment with corporate objectives. Use this framework to guide data collecting and case study analysis.

Data Collection Techniques: Gathered information for the case studies, employed a variety of techniques, including as document analysis, interviews, and observation. For learning purpose about the banks' AD implementation plans, infrastructure setups, migration procedures, performance indicators, security controls, and user experiences.

Finding Potential Banks Start by determining which Ethiopian banks have integrated Active Directory into their IT systems. To represent a wide range of deployment situations, banks with varying sizes, structures, and technological capabilities should be taken into account.

Variability in Models of Deployment: has been seek out banks that have implemented AD using various models, such as cloud-only, on-premise-only, and hybrid—which combine cloud and on-premise components. This variety makes it possible to compare all of the benefits, difficulties, and results related to each strategy in detail.

**Ethiopian Banking Industry:** Banks are an important sector in Ethiopia's economy, and they are likely to face a variety of IT infrastructure management demands and issues. This choice enabled the study to focus on the unique needs and issues of Ethiopian banks, generating insights that can be applied to the banking industry as a whole. The banks chosen as a sample are particularly significant since they are known to be early users of cloud computing and have been actively investigating its benefits, such as cost savings and increased scalability. This makes them a good case study for analysing Active Directory deployment strategies, which are an important part of IT infrastructure management.

The idea concentrated on the Ethiopian banking industry, which has been implementing cloud computing technologies to boost its digital transformation initiatives. Dashen Bank, for example, one of Ethiopia's pioneer banks, has used IBM Cloud Pack for Integration on Red

Hat to modernize its cloud integration architecture and grow its digital channels across any technological environment.

The research on cloud computing adoption challenges in the case of the Commercial Bank of Ethiopia can provide valuable insights into the specific challenges and issues faced by Ethiopian banks in adopting cloud computing solutions (Tesema, 2020).

Case Studies: Examine each chosen bank's case in-depth. This entails obtaining in-depth data regarding their Active Directory deployment, including their goals, obstacles encountered, tactics for implementation, and results.
Interviews: Hold interviews with important individuals at each bank, including network administrators, IT managers, security staff, and any other pertinent staff members engaged in the setup and upkeep of Active Directory.
Data collection: To assure dependability and triangulate your findings, use a variety of sources of information, including as interviews, documents (such as implementation plans and reports), and, if feasible, first-hand observations.
The number of participants should be sufficient to allow for a rich, in-depth understanding of the phenomenon, but small enough to support the meticulous, case-oriented analysis that is essential to qualitative inquiry, according to recommendations from experts in qualitative research. This justifies the sample size. It is anticipated that the planned sample size of 15–20 participants will reach data saturation, at which point the interviews will yield no new themes or insights.

### 3.4.1 Respondents Information

Fifteen respondents from the Information System (IS), Intranet department were chosen specifically for their knowledge relevant to the study's goal. The sample size for this study is based on 15 respondents with diverse employment classifications and descriptions:

| Business units | Respondent's job category | No. of respondent | Remark [CBE, BoA, AB, DB] |
|---|---|---|---|
| Information System [Intranet Team] | Manager | 3 | From all except AB |
| | Senior system administrator | 4 | From each bank |
| | System administrator | 5 | Two from CBE and the rest |
| | IS Officers | 3 | All except BoA |
| | Total | 15 | |

The data is collected from different governmental and private bank IT expertise.

- Sample Banks:

1. Commercial Bank of Ethiopia [CBE]
2. Bank of Abyssinia [BoA]
3. Dashen Bank [DB]
4. Awash Bank [AB]

### 3.5 Data Types and Sources

**A Cloud Computing Framework for the Ethiopian Banking Industry:** This source provides a framework for Ethiopian banks to implement cloud computing technologies, including hybrid cloud models.

**Embracing the Cloud for Banking:** This source examines the benefits and drawbacks of public, private, and hybrid cloud models for banks, including data residency, governance, security, control, and compliance.

**Cloud Computing Adoption Challenge in the Case of CBE:** This source gives insights on the obstacles and issues of cloud computing adoption, including as security, privacy, and bandwidth availability, which are pertinent to the proposal's focus on cloud deployment for Ethiopian banks.

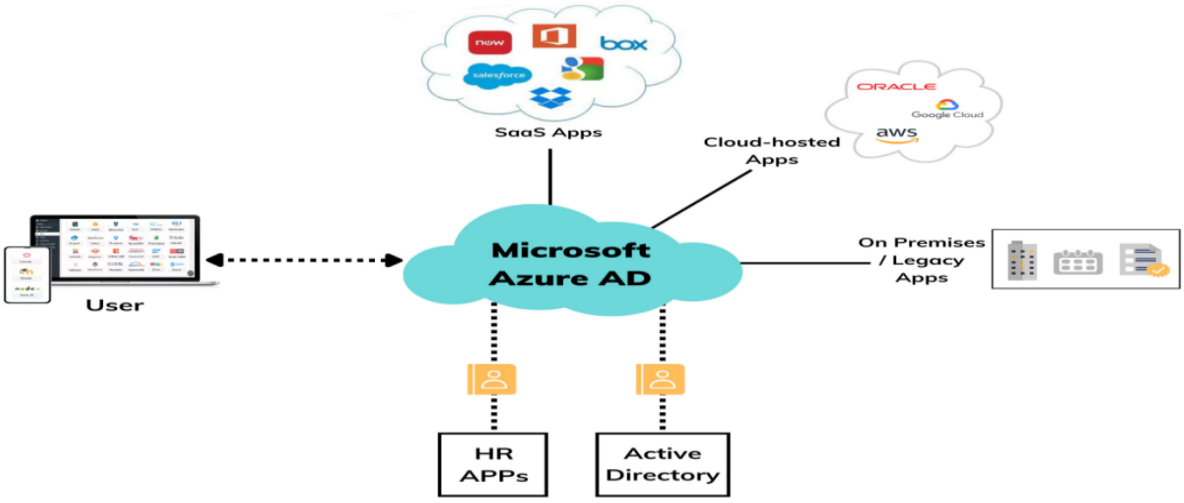



Figure 10. Microsoft Cloud deployment architecture

### 3.6 Data Collection Procedures

**Technical Data collecting:** Gathered technical insights into the implementation of Active Directory in various IT settings by using data collecting methods such as Azure Active Directory with Active Directory Sync to a Local Domain Controller.

Referring to industry resources such as AWS, Google cloud, and Microsoft Entra deployment plans to learn best practices, governance, and considerations for implementing Active Directory in hybrid situations.

The research acquired extensive insights into the parameters impacting the adoption of Active Directory in a hybrid, cloud environment and on-premises deployment for Ethiopian banks by utilizing these data collecting methodologies.

**Case Studies:** Investigated specific scenarios and issues, select a representative sample of Ethiopian banks of various sizes, kinds, and current IT infrastructure. Examined case studies of foreign banks who have already deployed Active Directory in a hybrid and cloud environment in order to extract best practices, issues encountered, and lessons learned.

There are two hypothetical instances of international banks that have used Active Directory in hybrid and cloud environments:

**Bank Horizon (Hybrid deployment):** a significant worldwide bank that operates in several countries. They have used a hybrid Active Directory deployment to match the necessity for centralized management with the ability to serve scattered offices and cloud-based services. In

this configuration, important identity management functions and sensitive data stay on-premise, while cloud services are used for scalability and collaboration tools.

Features: On-premise Active Directory Domain Controllers handle user authentication and access control for internal resources.

Azure Active Directory Connect synchronizes on-premise AD identities with Azure Active Directory (Azure AD), providing seamless access to cloud apps and services.

Hybrid Exchange setup integrates on-premise Exchange servers with Exchange Online in Office 365, offering unified email management and collaboration.

**Bank Alliance (cloud deployment):** a mid-sized multinational bank that has implemented a cloud-first strategy for its IT infrastructure. They relocated their whole Active Directory installation to the cloud to benefit from the scalability, agility, and cost reductions provided by cloud services. In this configuration, all authentication, access management, and directory services are hosted on cloud platforms.

Azure Active Directory (Azure AD) is the principal identity and access management platform, offering authentication and authorization services for on-premises and cloud resources.

Integration with the Microsoft 365 package provides easy access to productivity tools including Office applications, Teams, and SharePoint Online.

Azure AD B2B and B2C features are used to secure communication with external partners and maintain customer identities, respectively.

These examples show how international banks used Active Directory in hybrid and cloud settings to satisfy their distinct business and IT requirements. Whether they choose a hybrid approach to preserve control over vital services or a cloud-centric strategy for agility and scalability, these banks exhibit a wide range of deployment options adapted to their organizational objectives.

**Interviews and surveys:** have been conduct interviews and surveys with Ethiopian banks' IT professionals, decision-makers, and technical staff to learn about their present Active Directory implementation, problems, and considerations for implementing hybrid and cloud-based solutions from local bank employees and from vender consultants.

### 3.7 Ethical Consideration

**Data Security and Privacy:** When contemplating cloud or hybrid deployments, Ethiopian banks must ensure the security and privacy of their data. This involves adhering to data protection standards and protecting client information.

When conducting interviews or surveys, it was critical to gain informed permission from participants to ensure they understand the objective of study and how their data will be used.

**Transparency and Integrity:** The study performed in a transparent and ethical manner, ensuring that the findings are correctly portrayed and not modified to fit a certain narrative.

**Vendor Neutrality:** It is critical to preserve vendor neutrality and prevent any conflicts of interest that might impact the conclusions while acquiring information from industry resources and case studies.

By taking these ethical considerations into account, the proposal may guarantee that the study is carried out ethically and that the interests of Ethiopian banks and their stakeholders are prioritized.

### 3.8 Data Analysis

Identified reoccurring themes and patterns in your interview and focus group data using thematic analysis.

Categorized these themes to have a better understanding of the many viewpoints and experiences around Active Directory implementation.

**Analysis of narrative:** Concentrated on the interviewees' own tales and experiences.

Analyse these narratives to gain a better understanding of people's motives, concerns, and decision-making processes in relation to Active Directory implementation.

**Analysis of discourse:** Examined the language used in papers and interviews to gain a better understanding of the underlying power dynamics, beliefs, and values shared by various stakeholders.

This can provide light on potential conflicts of interest and hidden motives impacting Active Directory deployment decisions.

**Scenario Development**: Created future scenarios for the Ethiopian banking business, taking into account aspects such as economic development, regulatory changes, and technology improvements.

Examined how these scenarios affect the best Active Directory deployment approach for Ethiopian banks.

1. Transcription and Documentation: Started by transcribing all of your interviews verbatim. This entails transforming oral words into written text. To guarantee accuracy, use transcribing software or services whenever possible.

Documentation: Gathered and record all essential papers and artifacts pertaining to Active Directory deployment in the specified institutions. This contains implementation plans, reports, policies, and any other related documents.

2. Coding: Open Code carefully analysed each interview transcript and document to uncover concepts, themes, and patterns relevant to Active Directory implementation. This entails going through the data line by line, identifying and labelling relevant parts.

3. Theme Development: Use axial coding to uncover overarching themes in your data. Themes are patterns of meaning that run across the data and give insight into the study topics. Themes might include "security considerations," "cost effectiveness," "integration challenges," and so on. Sub-Themes: Within each primary topic, look for sub-themes or variants that offer depth and subtlety to your study. Sub-themes might be distinct difficulties or circumstances impacting the primary theme.

4. Mapping relationships: Investigated the links between various themes and subthemes. This entails understanding how certain elements (such as organizational size and IT infrastructure) impact deployment decisions.

Pattern Recognition: Looked for repeating patterns or trends in the Active Directory deployment tactics of various institutions. Compare and contrast these patterns to find similarities and differences.

5.Quotes and Illustrations: Choose illustrative quotations or excerpts from interview transcripts to support each topic and subtheme. These quotes serve as proof to back up your conclusions and provide depth to your research.

Used diagrams to depict the links between themes and sub-themes. This might help you convey your findings simply and concisely.

6.Theoretical Insights: Based on your theme analysis, evaluate how your findings connect to current ideas or frameworks about IT deployment techniques, such as technology adoption models or organizational theories.

New viewpoints: Investigate any new findings or viewpoints that come from your investigation. This might include practical ramifications, policy suggestions, or potential future research directions.

7. Validity and reliability: triangulate data from several sources (interviews, documents) and use member checking.

Improve dependability by keeping detailed documentation of your coding process, establishing consistency in data interpretation, and exchanging findings with peers or advisers to check interpretations.

8. Reporting Findings: Create a narrative explanation of your results that is organized around the identified themes and subthemes. Provide background, quotations, and examples to help explain each concept.

Discussion: Consider the significance of your findings in respect to the study questions and objectives. Compare your findings to current literature and ideas, emphasizing how your research adds to the area.

By taking this organized approach to data analysis, you can efficiently investigate and comprehend the subtleties of hybrid, cloud, and on-premise Active Directory implementation in Ethiopian banks, offering significant insights for both academic and practical applications.

# CHAPTER FOUR

# RESULT AND DISCUSSION

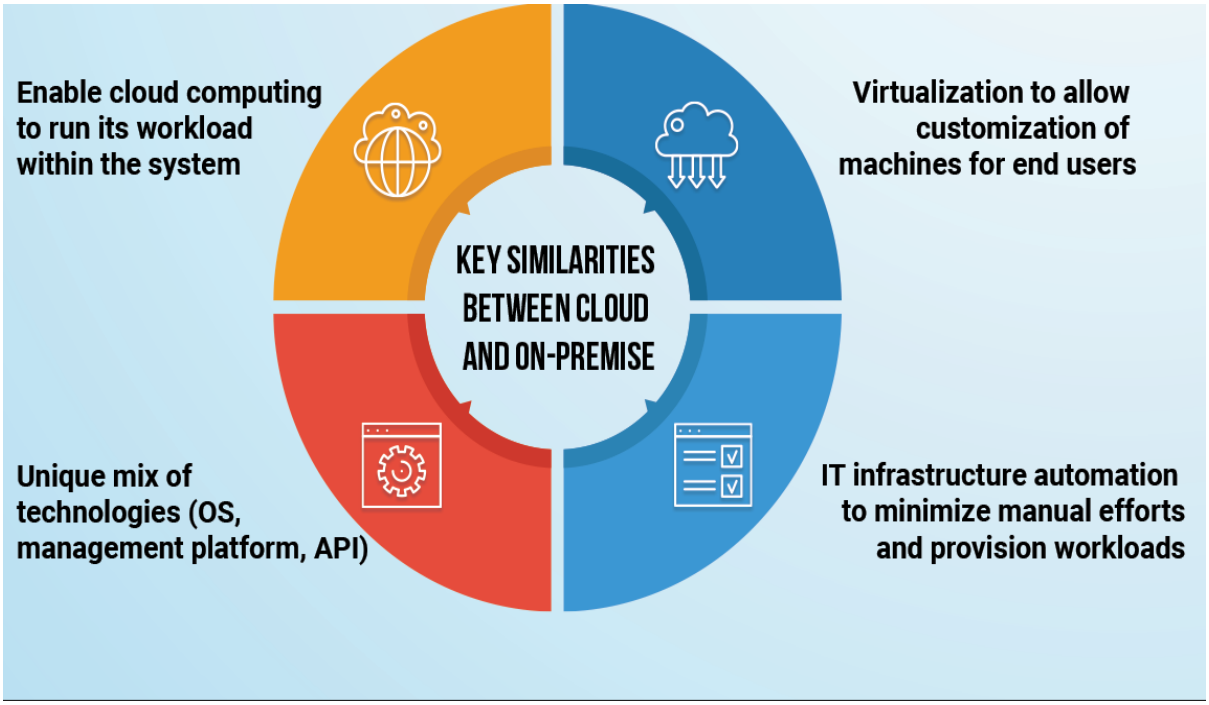
## 4.1 INTRODUCTION

The adoption of Active Directory (AD) in Ethiopia's banking industry is at a critical juncture, as institutions wrestle with the complexity of updating their IT infrastructure to meet changing operational demands while maintaining effective security and compliance controls. This section summarizes the findings of qualitative research undertaken to examine the efficacy and implications of hybrid, cloud, and on-premise Active Directory deployment methods in Ethiopian banks.

This research sought to provide comprehensive insights into the strategic considerations, operational challenges, and practical implications associated with each deployment model by combining in-depth interviews with IT professionals from various Ethiopian banks and detailed case studies of their IT infrastructures.

The following discussion delves into several key themes, including the motivations for selecting a deployment model, the operational and staffing implications, strategies for maintaining consistency in identity and access management across environments, and the broader implications for IT governance and security. By integrating these findings and doing critical analysis, we hope to contribute to a better understanding of the factors driving the adoption and implementation of Active Directory deployments in Ethiopian banks.

Furthermore, the discussion will look at the significance of our findings for the larger banking sector, drawing similarities with international best practices and emphasizing potential areas for further research and practical applications. Finally, this component provides a venue for reflection, analysis, and conversation, promoting informed decision-making and strategic planning among Ethiopian banks as they traverse the challenges of modern IT infrastructure implementation.




Figur11. Similarity of cloud and On-premise

## 4.2 Data Presentation

This study uses the popular theme analysis strategy for interpreting qualitative data, as suggested by Braun & Clarke (2019).

It entails finding themes in a collection of qualitative data so that inferences regarding the study questions can be made. Thus, research questions and the particular goals of this study are considered throughout analysis.

Thus, the following primary activities are completed in this study in order to conduct thematic data analysis, which is adapted from Braun and Clarke (2019).

To familiarize with data, interviews are recorded verbatim and saved in both digital and physical formats. Researchers read the transcripts numerous times to get a general comprehension of the data. Generating initial code: Initial codes are identified when the researcher has become acquainted with the data.

Search for themes: data is coded using an inductive approach, in which codes are derived from the data itself. The researchers meticulously organize previously established starting codes for ease of data inspection. The process involves grouping related beginning codes and identifying patterns across the dataset.

Review topics are determined by assigning descriptive labels to text parts relating to the research question and study objectives.

On-premises AD: Complete control over infrastructure and data necessitates specialized IT workers for administration and maintenance.

High upfront expenses for hardware and software; Limited scalability;

Cloud-based AD: Reduced IT strain and admin expenses; Scalability and flexibility.

Cloud storage raises security problems and relies heavily on internet access.

Hybrid AD: Combines advantages of on-premises and cloud installations.

Provides increased flexibility and catastrophe recovery options. Added complexity in maintaining two settings.

### 4.3 Data from Face-To –Face Interview

Inquiries regarding employees' data skills are made when interviewing survey respondents. This makes it easier to gauge how proficient staff members are with data. The individuals who answered the questions comprehend concepts connected to data.

The following is a presentation of the interviewers' observations regarding the data literacy of Banks' employees:

The managers personal opinions of different question about important variables that evaluated when deciding between a hybrid, cloud, or on-premises AD deployment in different perspective. Variables: security compliance, cost and scalability, user experience and productivity, infrastructure and technical requirement, Business continuity and disaster recovery, integration and interoperability, governance management and change management and user adoption were as follows:

Manager1: "*Security compliance: Compliance with regulatory requirements, such as data privacy and security standards. Ensuring secure data flow and access control across environments. Implementing robust security measures to prevent unauthorized access and data breaches.*

*Cost and Scalability: Evaluating the cost-effectiveness of each deployment model, considering factors like infrastructure, maintenance, and scalability. Assessing the ability to scale up or down as needed, ensuring seamless user experience and performance.*

*User Experience and Productivity: Ensuring seamless integration and single sign-on across on-premises and cloud resources. Maintaining consistent user experience and minimizing disruptions during migration or deployment.*"

Manager2: *"Infrastructure and Technical Requirements: Evaluating the technical capabilities of each deployment model, including network infrastructure, storage, and computing resources. Ensuring compatibility with existing systems and infrastructure.*

*Business Continuity and Disaster Recovery: Developing strategies for business continuity and disaster recovery in each deployment model. Ensuring minimal disruptions to operations and maintaining data integrity in the event of failures.*

*Integration and Interoperability: Assessing the ease of integration with existing systems and applications. Ensuring seamless communication and data exchange between on-premises and cloud environments. "*

Manager3: *"Governance and Management: Evaluating the management and governance requirements for each deployment model. Ensuring effective monitoring, maintenance, and updates across all environments.*

*Change Management and User Adoption: Developing strategies for change management and user adoption in each deployment model. Ensuring minimal resistance to change and effective training for users."*

The following are some suggestions made by selected senior system administrators concerning the costs and benefits of each deployment type, as well as the key cost drivers and possible savings:

Senior System Admin1: "*Cost Determination: • On-premises: Upfront costs will be a primary focus. This comprises hardware expenditures (servers and storage), Active Directory software licenses, and maybe additional security software, as well as continuing IT staff administration and maintenance costs.*

*Cloud-based Active Directory subscription and per-user fees will be evaluated. The data egress expenses if they routinely transfer data from the cloud.*

*Hybrid: A combination of on-premises and cloud costs. Interviewees would need to consider both, as well as the added complexity of managing a hybrid environment.*"

Senior System Admin2: "*Cost drivers include the amount of users and devices that require Active Directory authentication, which greatly affects license costs for both on-premises and cloud implementations.*

*On-premises deployments may require additional security software and staff expertise, increasing expenses. Cloud companies may include security elements in their subscription fees. Scalability: The ability to readily scale resources (users, storage) affects expenses. On-premises requires upfront hardware investments, whereas cloud provides on-demand scaling at possibly reduced upfront expenses.*"

Senior System Admin3: *"Potential Savings: • Cloud: Interviewees may identify potential savings in: Reduced hardware costs: No initial hardware purchases are required.*

*Lower IT staff workload: Cloud providers manage infrastructure, freeing your internal IT professionals to focus on other activities. Scalability benefits: Only pay for the resources you use. On-premises: Possible savings include: Avoiding vendor lock-in: Not dependent on a single cloud provider. Data control: Complete control over where data is stored."*

Senior System Admin4: "*Interviewees may underline the need for a Total Cost of Ownership (TCO) analysis that includes all costs over a given term (e.g., 3-5 years) to provide a comprehensive picture. This covers hardware, software, IT staffing costs, and even cloud subscription fees.*

*Interviewees may mention hidden expenditures, such as cloud deployment training or additional software licenses for on-premises security."*

By highlighting these issues, IT interviewees may demonstrate their ability to examine costs and possible savings across various deployment methods, allowing them to make an informed decision for their bank's needs.

Based on the search results, the important security and compliance issues for system administrator at Ethiopian banks are expected to include the following:

System Admin1: *"Regulatory Compliance: - Ensuring compliance with Ethiopian banking regulations and data privacy laws, including data protection, access controls, and audit trails. - Adhering to industry standards like PCI-DSS for secure payment card data handling. - Regularly reviewing and updating security policies and procedures to meet changing compliance requirements."*

System admin2: *"Data Security and Access Control: - Implement strong access*

*management and identity controls to prevent unauthorized access to sensitive data and systems. Providing safe data transmission and encryption between on-premises and cloud*

*environments in a hybrid paradigm. Regularly monitoring and auditing user actions and access privileges to identify and address security threats."*

System Admin3: *"Threat and Vulnerability Management: Proactively detect and manage security vulnerabilities across IT infrastructure, including on-premises and cloud components. Implementing effective security measures, such as firewalls, intrusion detection prevention systems, and SIEM tools. Providing security awareness training to staff to prevent insider threats and social engineering assaults."*

System Admin4: *"Business Continuity and Disaster Recovery: • Develop backup and recovery plans to assure data integrity and availability in case of system failures or disaster. Testing and upgrading business continuity and disaster recovery plans to verify effectiveness."*

System Admin5: *"Governance and Oversight: Define roles, responsibilities, and accountability for security management within the company. Conducting regular security audits and compliance assessments to detect and resolve weaknesses. Implementing effective communication and collaboration among IT, security, and business teams to align security measures with company goals.*
*Ethiopian banks can maintain data security and regulatory compliance by addressing five critical security and compliance requirements, regardless of whether they implement Active Directory in the cloud, on-premises, or hybrid mode."*

Interviewees for the study comparing hybrid, cloud, and on-premise Active Directory deployment asked for IS Officers in Ethiopian banks are likely to respond with specific implications for IT operations, staffing needs, and the IT team's skills, duties, and responsibilities. Below is a breakdown of replies for each deployment model:

IS Officer1: *"On-Premise implementation: IT operations: On-premise implementation may necessitate dedicated hardware, infrastructure, and maintenance, thus increasing operational expenses and resource allocation for the IT team.*
*Additional IT professionals may be required to manage and maintain the on-premise infrastructure, including network administrators, system engineers, and security personnel.*

*Impact on IT staff abilities, roles, and responsibilities: IT team members would require specialized skills for maintaining on-premise servers, resolving hardware issues, and assuring*

*data protection on the physical premises. Their responsibilities may include server maintenance, backups on a regular basis, and security protocol implementation."*

IS Officer2: *"Cloud Deployment: IT operations: Offloading hardware management to a cloud provider can reduce expenses and improve scalability*.

*- Staffing requirements: While fewer IT professionals may be required for hardware maintenance, more personnel may be required to manage cloud resources, monitor performance, and ensure compliance with cloud service agreements.*

*- Impact on IT team skills, tasks, and responsibilities: IT team members would require knowledge of cloud technologies such as AWS, Azure, and Google Cloud Platform.*

*Their responsibilities may include providing and maintaining cloud resources, enhancing performance, and guaranteeing data security in the cloud environment."*

IS Officer3: *"Hybrid Deployment: IT operations: Hybrid deployment mixes on-premise and cloud resources to provide flexibility and scalability while maintaining control over sensitive data.*

*Staffing requirements: Hybrid deployment may necessitate a wide skill set within the IT staff to successfully handle both on-premise and cloud components.*

*Impact on IT staff skills, tasks, and responsibilities: IT team members will require a mix of on-premise and cloud competence. Their responsibilities may include integrating on-premise and cloud systems, establishing hybrid identity management solutions, and ensuring data consistency and security across many settings."*

In conclusion, interviewers would likely underline the need of matching IT operations, personnel requirements, and skill development with the chosen deployment architecture to guarantee successful Active Directory implementation and maintenance inside Ethiopian banks. They may also highlight the importance of continual training and adapting to new technologies and industry best practices.

Address the problems and techniques for ensuring that identities, access, and privileges are consistent across IT environments. Here is a breakdown of possible responses from employee in different profession level:

Manager1: *" Identities, access, and privileges are consistent.*

*Integration and synchronization tools: Interviewees may mention using identity management solutions, such as Microsoft Azure Active Directory Connect or third-party identity synchronization tools, to keep user identities and attributes consistent across on-premise and*

*cloud environments.*

*Single-sign-on (SSO) solutions: Implementing SSO solutions such as Azure Active Directory (AAD) or Active Directory Federation Services (ADFS) allows users to access both on-premise and cloud services with a single set of credentials, resulting in a more seamless experience while maintaining security. Role-based access control (RBAC): RBAC rules can be used to design and enforce consistent access privileges for users across all environments, ensuring that employees have the necessary access levels based on their jobs and responsibilities."*

Senior System Admin1*: "Continuous monitoring and auditing: Regular monitoring and auditing of access rights and permissions aids in the detection and resolution of discrepancies or unwanted access attempts, ensuring the integrity of identity and access management processes across all deployment models.*

*Identity Lifecycle Management Methods and Tools:*

*Provisioning and deprovisioning workflows: Interviewees may highlight the necessity of automating the process of provisioning user accounts and resources, as well as deprovisioning accounts as soon as individuals leave the organization or change jobs. Tools like AAD Premium, Okta, and SailPoint Identity Now enable you to manage the whole identity life cycle."*

System Admin1: *"Self-service portals: Allowing users to seek access permissions, reset passwords, or update their profile information can help to streamline identity management operations and minimize the workload on IT workers. Users can manage their identities and access rights autonomously using solutions such as Azure AD self-service password reset and the MyApps site. Identity governance frameworks and solutions can help enforce policies and compliance requirements for identity management, access control, and privileged account management. Solutions like SailPoint Identity IQ and IBM Security Identity Governance and Intelligence (IGI) allow you to define, enforce, and audit identity governance policies"*

To summarize, respondents would likely underline the necessity of implementing strong identity and access management strategies, supported by appropriate tools and technologies, to maintain consistency and security across Ethiopian banks' on-premise, cloud, and hybrid IT infrastructures. They may also emphasize the importance of continuous monitoring, automation, and compliance procedures to manage increasing security threats and regulatory requirements.

### 4.4 Data from Observation case study

The organizations properly analyze their individual needs and objectives before making any decisions. Security, scalability, cost-effectiveness, and existing IT infrastructure are all important factors to consider. Furthermore, it is critical to stay current on industry rules and compliance requirements to ensure that the chosen deployment strategy fulfills all essential criteria. Furthermore, organizations to use hybrid deployment methods whenever possible, as they provide the flexibility to combine on-premises and cloud-based solutions to satisfy a variety of business requirements. This method allows enterprises to strike a balance between security, scalability, and cost-efficiency.

**Assess present Needs:** The significance of thoroughly examining the organization's present needs and future growth goals prior to making any decisions. Understanding the exact requirements will assist in selecting the most appropriate deployment model.

**Consider Cloud Solutions:** Given the growing popularity of cloud technologies, several studies recommend cloud-based Active Directory solutions. They may highlight advantages like as scalability, flexibility, and lower infrastructure costs. Others may advise a hybrid approach, which combines on-premises and cloud-based technologies. This enables enterprises to get the benefits of both environments while also addressing security and regulatory issues.

**Security Considerations:** Security is frequently a major consideration for businesses. Many studies focused on the significance of selecting a deployment architecture that prioritizes security features and compliance needs including data encryption, access controls, and auditing capabilities.

Another topic for debate is employee user experience and accessibility, particularly in remote or distributed work situations. The recommend deployment options may allow for seamless access to resources from any location and on any device. Scalability and performance are critical considerations, especially for growing enterprises. The research suggests selecting a deployment approach that can readily grow to handle a rising number of users and devices while maintaining performance.

**Expertise and Support:** The organization's internal expertise and the availability of external support resources may also be highlighted. Some documents emphasize advocate selecting a deployment strategy that is compatible with the organization's technological capabilities and gives access to dependable support services.

**Migration Strategy:** The documents underline the need of a well-planned migration strategy for organizations wishing to change their existing Active Directory setup. This involves identifying dependencies, limiting downtime, and maintaining data integrity during the move.

**Vendor Evaluation:** Lastly, the collected data advise carefully assessing the various suppliers and products on the market. This entails taking into account elements including product features, cost, long-term road map, and vendor reputation.

**Regulatory Compliance:** The importance of regulatory compliance in the banking sector, highlighting that, regardless of deployment architecture, adherence to industry rules such as PCI DSS, GDPR, and others is critical. They might explain how each deployment model necessitates certain compliance measures, and how banks must guarantee that their security policies comply with these rules.

**Risk assessment and mitigation:** Observed cases highlight how banks undertake detailed risk assessments to identify potential security concerns associated with different deployment architectures. Data Protection: Data protection is a major concern for banks, and respondents may discuss the steps taken to safeguard sensitive client information across various deployment architectures. They may discuss encryption mechanisms, access controls, and data loss prevention tactics used to protect data both on-premises and in the cloud.

**Identity and Access Management (IAM)** is an important part of security in the banking business, that we describe how banks handle user identities and access privileges across various deployment architectures. They may emphasize the significance of implementing strong IAM solutions to ensure that only authorized users have access to sensitive systems and data, regardless of deployment architecture. Security Monitoring and Incident Response: The researchers underline the need of ongoing security monitoring and timely incident response in the banking sector. They may describe how banks utilize advanced security tools and technologies to detect suspicious activity and respond promptly to security issues, regardless of whether the infrastructure is on-premise, cloud-based, or hybrid.

**Vendor Management:** In cloud-based deployment topologies, the related journals address the significance of vendor management in assuring security. They might explain how banks carefully select cloud service providers, analyze their security capabilities, and create clear contractual agreements to reduce the risks associated with third-party services. Employee Training and Awareness: This profession expertise discuss on their articles the importance of employee training and awareness initiatives in ensuring security across various deployment architectures. They could address how banks educate their staff about security best practices, phishing scams, and other security issues in order to prevent breaches and illegal access.

**Adaptive Security Measures:** Finally, related files explain the importance of adaptive security measures that can adjust to changing threats and settings. They might discuss how banks utilize technologies like machine learning and behavioral analytics to detect and respond to new security threats across a variety of deployment models.

Handling user IDs and access controls across many deployment modes (on-premise, cloud, and hybrid) necessitates a comprehensive approach to identity and access management (IAM). Here's how corporations normally handle this:

Many organizations employ a centralized identity management system, such as Microsoft Active Directory (Active Directory) or LDAP (Lightweight Directory Access Protocol), to handle user IDs and access controls across many deployment models. This centralization assures uniformity and ease of management regardless of where resources are located.

**Single Sign-On (SSO):** SSO solutions enable users to authenticate once and access various resources across different deployment modes without having to log in to each system individually. This improves the user experience while lowering the danger of password fatigue and security issues.

**Role-depending Access Control (RBAC):** Users are granted permissions depending on their responsibilities within the organization. Organizations may enforce consistent access controls across on-premise, cloud, and hybrid environments by centralizing role definitions and permissions.

**Integration with Cloud Identity Providers:** In cloud deployments, enterprises frequently link their on-premise identity management systems with cloud identity providers such as Azure Active Directory, AWS Identity and Access Management (IAM), and Google Cloud Identity. This integration enables easy authentication and authorization across hybrid environments.

**Federated Identity Management (FIM)** allows users to use their existing credentials to access resources across domains or contexts. This is especially important in hybrid deployments, where users must access both on-premise and cloud resources with a single set of credentials. Attribute-Based Access Control (ABAC): ABAC uses numerous qualities connected with people, resources, and environmental elements to generate dynamic access control choices. This technique enables granular access control based on contextual parameters, which is useful in complex deployment settings.

**API Access Management:** In cloud and hybrid environments, enterprises frequently use API access management solutions to automate access to cloud services and resources. This enables secure integration of on-premises systems and cloud services while imposing access controls.

**Auditing and monitoring:** Regardless of the deployment strategy, companies must build effective auditing and monitoring tools to track user actions and access attempts. This aids in the detection and mitigation of security events, as well as assuring regulatory compliance.

The cost of configuring and maintaining an Active Directory (AD) deployment model varies depending on several factors, including the organization's size, the complexity of the environment, the deployment model chosen (on-premise, cloud, or hybrid), and the level of automation and outsourcing involved. Here's a breakdown of the possible costs:

**Initial Configuration Costs:**

**Hardware and software:** For on-premise implementations, enterprises must spend in hardware infrastructure such as servers, storage, and networking devices. In addition, obtaining licenses for the Windows Server operating system and Active Directory services incurs software expenditures.

**Consulting Services:** Organizations may choose to employ consultants or professionals to help with the initial setup and configuration of the Active Directory environment, particularly if they lack in-house experience. Ongoing maintenance costs include staffing resources for administering and maintaining the Active Directory environment. This contains functions like user provisioning, group management, security monitoring, and troubleshooting.

**Software Updates and Patch Management:** Regular updates and patches are required to keep the Active Directory environment secure and up to date. Depending on the deployment model, businesses may need to set aside resources for testing and deploying updates to on-premise servers, as well as managing updates in cloud settings.

Backup and disaster recovery solutions are critical for data protection and company continuity. Backup software licenses, storage infrastructure, and remote replication for disaster recovery may all cost money.

Organizations can invest in security technologies and services, such as antivirus.

**Cloud Deployment Costs :**

**Subscription costs:** Cloud-based Active Directory services like Azure Active Directory or AWS Directory Service often charge subscription costs based on consumption, such as the number of users or directory objects.

**Data Transfer Costs:** Cloud providers may charge for data transfers between on-premise and cloud environments, particularly in hybrid installations that involve data replication and synchronization.

**Third-party Tools and Services:**

Organizations may wish to invest in third-party tools and services to improve the functioning and management of their Active Directory system. This could include solutions for identification and access management, auditing and compliance, and automation and orchestration.

Overall, the expenses of designing and maintaining an Active Directory deployment model can vary greatly depending on the organization's individual needs, preferences, and distribution method. Organizations must thoroughly analyze their needs and budget limits before making judgments about their Active Directory implementation plan.

Banks frequently integrate with other systems and applications across different deployment types (on-premise, cloud, hybrid) using a mix of methods and technologies to ensure smooth communication, data exchange, and security. Here's how they normally handle integration:

**API-Based Integration:**

Banks are increasingly relying on APIs (Application Programming Interfaces) to help integrate systems and applications. APIs enable standardized communication and data sharing across diverse systems, regardless of deployment model.

Banks can create their own APIs or use third-party APIs supplied by vendors and service providers to interact with banking platforms, payment gateways, customer relationship management (CRM) systems, and other applications.

**Middleware and integration platforms:**

Middleware solutions and integration platforms equip banks with tools and frameworks for orchestrating and streamlining the integration process. These systems enable a variety of integration patterns, including message queuing, data transformation, and service mediation.

Banks can use middleware solutions on-premise, in the cloud, or in a hybrid environment to connect legacy systems to new applications and services.

**Service Oriented Architecture (SOA):**

SOA principles Advocate for modular, loosely connected services that can be readily integrated and reused across multiple systems and applications. Banks may use SOA to design and deploy a flexible integration architecture that promotes agility and scalability.

SOA enables banks to expose essential banking activities as services that can be accessed by internal systems, external partners, and third-party developers through APIs.

**Event Driven Architecture (EDA):**

EDA allows for real-time integration and event-driven communication between systems and applications. Banks can use event-driven messaging solutions like Apache Kafka or RabbitMQ to publish and subscribe to events across different deployment scenarios.

EDA enables banks to respond swiftly to business events, automate procedures, and synchronize data across systems in a timely manner.

**Data Integration and ETL Tools:**

Banks use data integration and ETL (Extract, Transform, and Load) solutions to harmonize and consolidate data from various sources. These solutions allow banks to cleanse, modify, and enrich their data before feeding it into target systems and data warehouses.

Banks can use data integration and ETL solutions on-premises or in the cloud to provide batch processing, real-time data streaming, and data synchronization across deployment types.

**Security and Compliance Considerations:**

Banks put security and compliance first when interacting with other systems and apps. They use encryption, access restrictions, and identity management solutions to safeguard sensitive information and maintain regulatory compliance.

Banks conduct extensive risk assessments and security audits to discover and address security flaws across integration points and data flows.

Overall, banks use APIs, middleware, architecture patterns, and integration technologies to easily interface with other systems and applications across various deployment models while meeting security, regulatory, and performance requirements.

The scalability of an Active Directory implementation varies according to the deployment model (on-premises, cloud, or hybrid). Here is how scalability usually differs between different models:

**On-premises deployment:**

Scalability in on-premises Active Directory implementations is constrained by the actual hardware infrastructure, like as servers, storage, and network bandwidth, that enterprises have in their data centers.

Scaling an on-premises Active Directory operation frequently necessitates the provisioning of extra hardware resources, such as domain controllers, to manage increased user authentication, directory lookup, and replication traffic.

While enterprises have complete control over their on-premises infrastructure, scaling may

require upfront capital investments as well as lead times for new hardware acquisition, installation, and configuration.

**Cloud Deployment:**

Cloud-based Active Directory services, such as Azure Active Directory (Azure Active Directory) and AWS Directory Service, provide better scalability than traditional on-premises deployments.

Cloud providers manage the underlying infrastructure and automatically scale resources based on demand, allowing businesses to quickly expand capacity as needed.

Scalability in cloud-based Active Directory services is achieved by horizontal scaling, which involves dynamically provisioning extra domain controller instances to disperse work load and manage increased authentication and directory queries.

Organizations can scale resources up or down based on usage patterns and pay only for the resources they use, resulting in more cost-effective scalability than on-premises implementations.

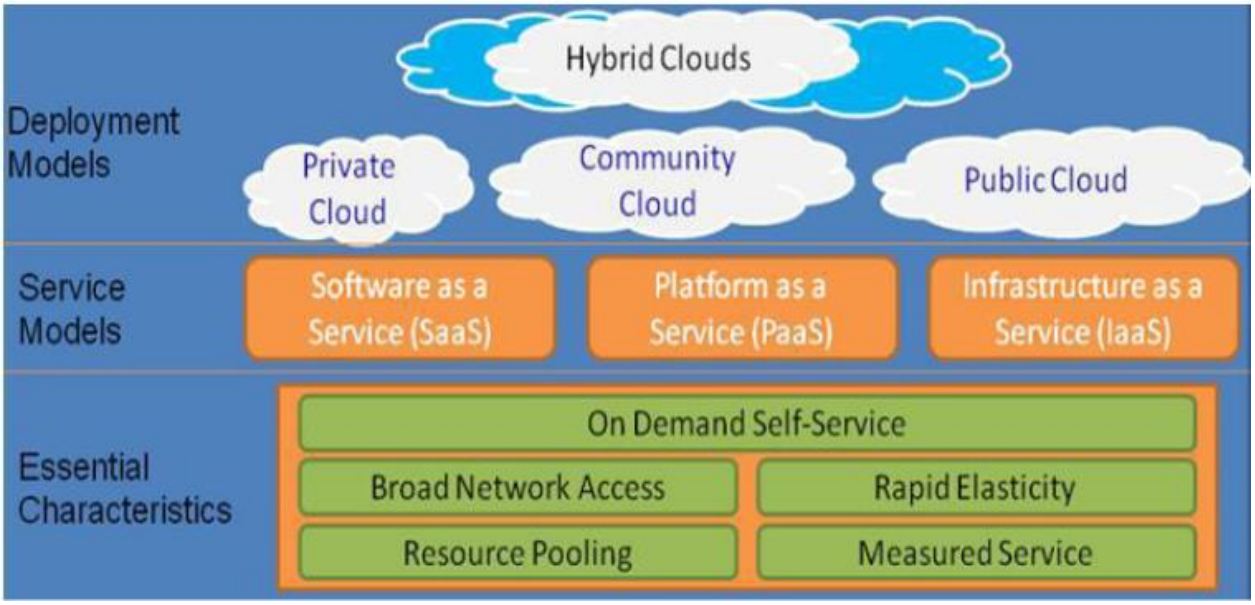



Figure 12. NIST Cloud Definition Framework

**Hybrid deployment:**

Hybrid Active Directory installations integrate on-premises and cloud-based Active Directory services, allowing businesses to reap the scalability benefits of both deployment methods.

In a hybrid deployment, enterprises can expand their on-premises Active Directory environment to the cloud by syncing user identities, groups, and credentials between on-premises Active Directory and Azure Active Directory.

This hybrid strategy allows enterprises to benefit from the scalability and agility of cloud-based Active Directory services while still integrating with their existing on-premises infrastructure and applications.

Organizations can extend their hybrid Active Directory system by changing the synchronization configuration, adding Azure Active Directory Connect servers, or allocating more cloud resources to accommodate increased workload or directory synchronization traffic.

Overall, on-premises Active Directory installations necessitate manual provisioning and scaling of physical resources, whereas cloud-based Active Directory services provide better scalability and flexibility, with the ability to dynamically scale resources in response to demand. Hybrid Active Directory implementations strike a mix between the cloud's scalability benefits and the integration capabilities of on-premises infrastructure.

A bank's Active Directory deployment requires strong backup and disaster recovery techniques to assure data integrity, business continuity, and regulatory compliance.

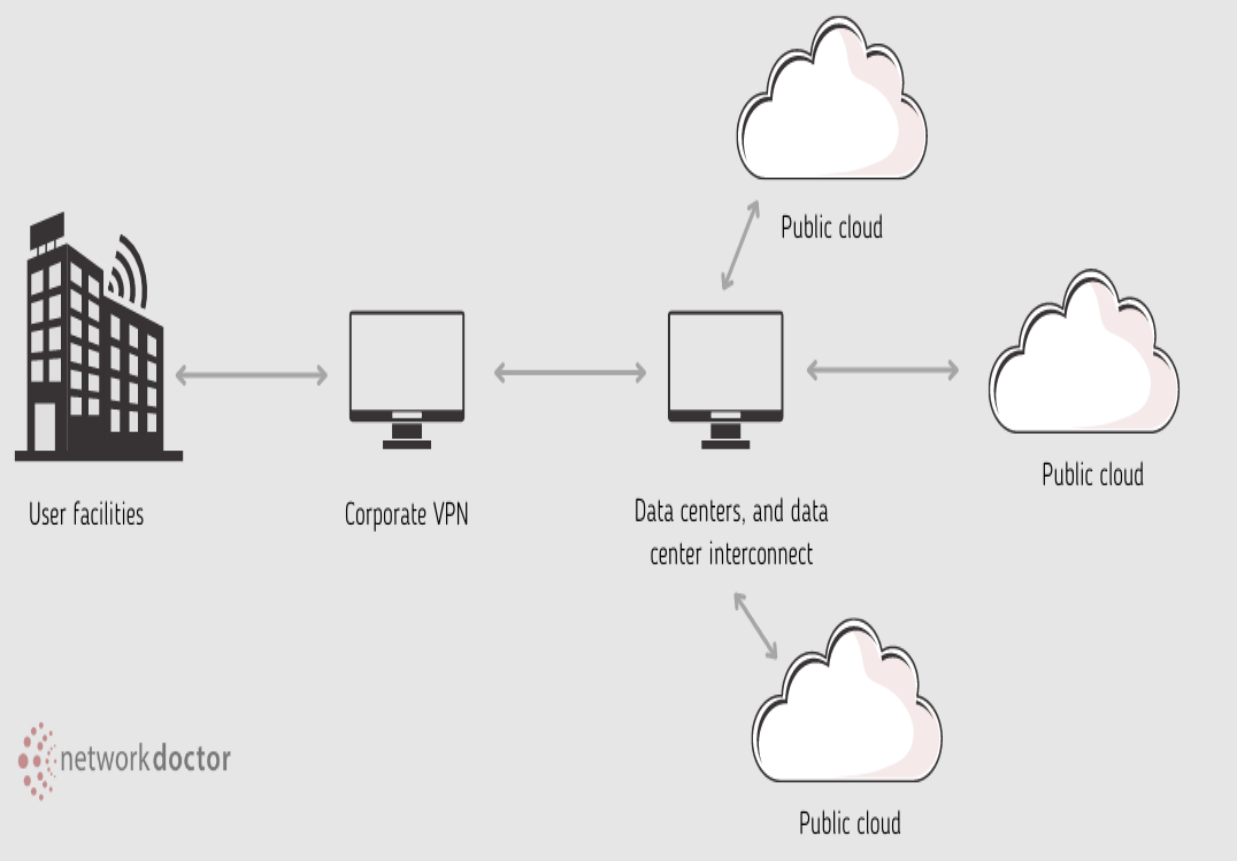



Fig 13. Physical view of optimal hybrid cloud network

Here's how most banks approach backup and disaster recovery for their Active Directory environment:

**Backups occur on a regular basis.**

Banks make regular backups of their Active Directory database, which contains user accounts, group memberships, organizational units (OUs), group policies, and other configuration information.

Backup frequency varies according to the bank's risk tolerance, but daily or weekly backups are usual to reduce data loss in the event of a crisis.

**Off-Site Storage:**

Banks keep backup copies of their Active Directory data in safe offsite locations, separate from the central data center. Offsite storage provides protection against localized disasters such as fire, flood, and physical damage to core infrastructure.

Some banks use cloud-based backup systems for remote storage, exploiting the scalability and redundancy of cloud storage providers.

**Redundancy and High Availability:**

Banks install redundant domain controllers in several physical locations to ensure that Active Directory services are highly available. Redundancy reduces the impact of hardware or network failures on Active Directory operations.

Load balancing and fail over procedures are used to distribute authentication requests and directory queries across redundant domain controllers, and traffic is automatically redirected in the event of failure.

**Disaster Recovery Plans:**

Banks create detailed disaster recovery plans that outline methods for restoring Active Directory services and data following a severe outage or disaster.

Disaster recovery plans include clearly defined roles and duties, communication protocols, escalation procedures, and step-by-step directions for starting recovery operations.

Banks perform regular disaster recovery drills and simulations to ensure that their plans are effective and that they are prepared to respond to various scenarios.

**Granular Recovery Options:**

Banks invest in backup solutions that enable granular recovery of Active Directory objects and properties. Granular recovery allows administrators to restore specific user accounts, group memberships, or group policies without restoring the entire Active Directory database.

This level of granularity reduces downtime and data loss by enabling for targeted recovery of individual items that have been accidentally deleted, corrupted, or changed without authorization.

**Monitoring and alerting:**

Banks use monitoring and alerting techniques to proactively discover problems with Active Directory replication, database integrity, and backup operations. Automated alerts advise administrators of potential issues, allowing for timely resolution to avoid data loss or service disruptions.

By implementing these backup and disaster recovery techniques, banks may reduce the impact of unforeseen events on their Active Directory environment, maintain operational resilience, and maintain the trust and confidence of customers and regulators in their ability to protect essential data and services.

## 4.6 Discussions

Here's a brief discussion for a thesis comparing hybrid, cloud, and on-premise Active Directory deployments in Ethiopian banks:

Many organizations, including banks, rely heavily on Active Directory (Active Directory) as part of their IT architecture. Ethiopian banks confront difficulty in effectively managing their Active Directory deployments because to variables such as changing financial rules, monopolized banking products, and out-of-date legislative frameworks. This thesis compares the advantages and disadvantages of hybrid, cloud, and on-premise Active Directory deployment models for Ethiopian banks.

**On-premises Active Directory**

On-premises Active Directory gives Ethiopian banks complete control over user accounts, security rules, and access privileges. This is crucial for highly regulated industries like banking, which have strong compliance requirements for data security and privacy.

On-premises Active Directory enables integration with traditional banking systems that may not be compatible with cloud services.

On-premises Active Directory involves significant infrastructure and operational overhead, making it pricey for banks. It has limited scalability compared to cloud-based solutions.

**Cloud Active Directory**

Cloud Active Directory, a cloud-based IAM service, provides various benefits to Ethiopian banks wishing to modernize their identity management.

It interacts effortlessly with Microsoft 365 and other cloud services, which banks are increasingly using.

Cloud Active Directory is extremely scalable to handle rising cloud environments and mobile/remote users. Banks can shift infrastructure management to Microsoft. However, some advanced Active Directory functions might not be available with Cloud Active Directory.

Banks may be concerned about keeping sensitive financial data on public clouds due to compliance problems.

**Hybrid Active Directory**

Ethiopian banks can extend their on-premises Active Directory identities to the cloud using a hybrid Active Directory implementation that uses Cloud Active Directory Connect.

This allows banks to progressively shift to the cloud while maintaining control over crucial on-premises resources. Hybrid Active Directory provides a single sign-on for both on-premises and cloud apps. However, managing two IAM systems is more complex. Banks would still rely. Ethiopian banks should carefully examine their current infrastructure, regulatory compliance requirements, security demands, scalability objectives, and administrative overhead before deciding which Active Directory to use.

Many banks may benefit from a hybrid solution, which allows them to extend Active Directory to the cloud while keeping control over critical data and legacy applications.

However, institutions with stringent regulatory needs and low cloud penetration may need to stay on-premises. Finally, the choice is determined by each bank's unique requirements and risk tolerance. Hybrid Active Directory emerges as a promising transitional option that allows banks to leverage the cloud while still maintaining the control and compliance they require.

The search results form a good platform for analyzing the tradeoffs between control, security, cost, and management overhead for each Active Directory deployment model in the Ethiopian banking industry.

**Hybrid cloud deployment.**

Dashen Bank modernized its IT infrastructure and accelerated its digital transformation by using a hybrid cloud solution based on Red Hat OpenShift and IBM Cloud Pak.

Dashen Bank's hybrid strategy enables the deployment and expansion of digital channels in both cloud and on-premise environments, boosting open banking with partners like fintech’s and telecom firms.

Ethiopian banks benefit from hybrid cloud technology, which offers agility, security, and quick time-to-market for integrating new apps and partners.

Based on the sources supplied, a discussion of hybrid, cloud, and on-premise Active Directory deployment in the context of Ethiopian banks can be synthesized:

Ethiopian institutions, like Dashen Bank, have adopted hybrid cloud solutions to upgrade their IT infrastructure and improve digital transformation.

Dashen Bank worked with IBM to build IBM Cloud Pak for Integration on Red Hat Open Shift, allowing them to grow digital channels and improve client services.

The hybrid cloud model enables agility, security, and faster time-to-market for new apps and collaborations, including open banking initiatives with fintech's and telecom businesses.

**Challenges in Cloud Adoption:**

The high cost of cloud services, along with unstable internet connectivity in Ethiopia, make it difficult for SMEs, particularly banks, to fully shift to the cloud.

A lightweight hybrid cloud approach, in which basic services are used via the cloud while key systems remain on-premise, can be a cost-effective solution for Ethiopian banks with limited infrastructure and connection.

**On-premise Deployment:**

Many Ethiopian banks initially choose for on-premise implementation due to the high costs associated with cloud services and the necessity to assure e-banking service availability despite frequent power and phone outages.

# CHAPTER FIVE

# CONCLUSION, RECOMMENDATIONS AND FUTURE WORKS

## 5.1 Conclusion

The thesis investigated AD deployment in Ethiopian banks, focusing on the comparative analysis of hybrid, cloud, and on-premise models. Using qualitative methods such as interviews with IT professionals and case studies of bank IT infrastructures, several significant findings were revealed, shedding light on the complexities and considerations involved in selecting the most appropriate deployment model.

One of the study's key conclusions is the recognition of Ethiopian banks' various IT infrastructure needs and goals. While some institutions prefer the flexibility and scalability of cloud deployment, others value the control and security of on-premise solutions. Hybrid deployment emerged as a balance between these two extremes, reflecting the complex approach required to solve each bank's particular difficulties. When deciding on the best Active Directory deployment strategy, Ethiopian banks should carefully analyze their IT requirements, including scalability, security, cost-effectiveness, and regulatory compliance.

Ethiopian banks benefit from hybrid cloud solutions, which combine on-premises infrastructure with public and private cloud environments. This strategy enables banks to maintain control over sensitive data while taking advantage of cloud computing's scalability and cost-efficiency.

When it comes to embracing cloud technologies, Ethiopian banks continue to prioritize security and compliance. Banks must verify that their cloud suppliers follow tight security measures and regulatory guidelines. Application-level encryption can give an extra degree of security for critical data.

Cloud adoption is gaining traction among banks throughout the world, driven by the demand for scalability, agility, and the opportunity to leverage the power of data and emerging technologies. However, the transition to the cloud is difficult, particularly for banks that have considerable investments in on-premises infrastructure.

Ethiopian banks should thoroughly assess their individual requirements and create a cloud adoption strategy that is aligned with their business objectives and risk appetite. A hybrid approach that takes advantage of both on-premises and cloud environments may be the best choice for many Ethiopian banks.

Ethiopian banks may retain consistent identities, access, and privileges across on-premises and

cloud resources by deploying Active Directory using a hybrid cloud architecture. This can be accomplished by implementing single sign-on solutions, directory services integration, cloud IAM tools, and privileged access management systems.

The findings presented herein provide significant insights and recommendations to support decision-making processes in the banking industry, facilitating the adoption of IT infrastructures that correspond with business objectives and operational requirements.
As technology evolves and regulatory contexts change, constant research and adaptation will be required to ensure the resilience and efficacy of Active Directory deployments in Ethiopian banks and other comparable companies worldwide.

## 5.2 Recommendation

Based on the information gathered from viewing the case studies, the following recommendations for this study would be:

**1. Incorporate Cloud Security Frameworks**: Given the growing adoption of cloud computing and the security concerns raised in the research, it is recommended that established cloud security frameworks, such as those proposed by the Cloud Security Alliance (CSA) or the International Organization for Standardization (ISO), be integrated to improve the security of Active Directory deployments in Ethiopian banks.

**2. Address Data Compliance and Governance**: Focus on resolving the primary security concerns highlighted by Cloud Service Consumers (CSCs), such as data compliance, legal challenges, and data governance loss. Create strategies inside Active Directory deployment models to guarantee that data compliance and governance are properly managed.

**3. Consider Billing and Commercial Complexity:** Recognize that hybrid cloud installations are more difficult in terms of billing and commercialization than other models. Assess the impact of this complexity on cost management and financial planning in the context of Ethiopian banks.

**4. Prioritize security concerns:** when comparing deployment methods, based on the security risks identified in the research. Address security concerns unique to each deployment type, emphasizing the significance of strong security measures in the banking industry.

**5. Assess Transparency and Governance:** Evaluate each deployment model's transparency and governance features, paying special attention to data compliance, legal challenges, and governance. Examine how each model promotes openness and regulatory compliance in the Ethiopian banking industry.

**6. Propose a comprehensive security framework:** Create a comprehensive security

framework that combines IT governance concepts to solve security issues in hybrid, cloud, and on-premises deployments. Ensure the framework includes comprehensive security safeguards, compliance systems, and resource management techniques specific to the banking industry.

**7. Validate the suggested security framework:** stakeholders such as IT specialists and employees from Ethiopian banks collect input on the framework's efficacy in solving security problems for Active Directory installations in banking.

**8. Benchmark Against Industry Standards:** Examine how well-established cloud security frameworks, such as those advised by the International Organization for Standardization (ISO) or the Cloud Security Alliance (CSA), compare to the proposed security framework. Make sure the framework complies with industry standards and best practices for cloud security in financial institutions.

You can offer important insights into the challenges, security considerations, and governance elements related to hybrid, cloud, and on-premises deployments in the banking industry by implementing these recommendations into your study on Active Directory deployment models in Ethiopian banks.

## 5.3 Future Works

1. **Cost Analysis and Optimization:** Conduct a detailed cost analysis comparing the expenses associated with hybrid, cloud, and on-premises Active Directory deployments in Ethiopian banks. Explore strategies for optimizing costs while maintaining security and efficiency.

**2. Enhanced Security Measures:** Investigate advanced security measures and technologies that can be implemented to address the security concerns highlighted in the research. Focus on enhancing data compliance, legal issues, and governance to ensure robust security in all deployment models.

**3. Integration of IT Governance:** Explore the integration of IT governance principles into the deployment of Active Directory across different models. Develop frameworks that align with IT governance best practices to enhance transparency, resource management, and compliance within Ethiopian banking institutions.

**4. Stakeholder Engagement:** Engage key stakeholders, including IT professionals, banking executives, and regulatory bodies, to gather insights on the challenges and opportunities associated with different deployment models. Incorporate feedback to tailor future research and implementation strategies.

**5. Comparative Analysis with Industry Standards:** Conduct a comparative analysis of the proposed deployment models with industry standards and best practices, such as those recommended by the Cloud Security Alliance (CSA) and the International Organization for Standardization (ISO). Identify areas of alignment and potential areas for improvement.

By focusing on these areas for future research, you can further enhance the understanding of Active Directory deployment models in Ethiopian banks, address key challenges, and develop strategies to optimize security, cost-effectiveness, and governance in IT infrastructure management.

# APPENDIX

## Survey questions and sample interview questions

1. What factors influenced your decision to choose which deployment model for Active Directory in Ethiopian banks business?
2. What advice would you give to enterprises considering choosing or modifying their Active Directory deployment model?
3. In terms of security, how does in bank industry manage the distinct needs of each deployment architecture (on-premise, cloud, hybrid)?
4. How do you handle user IDs and access controls across different deployment modes (on-premise, cloud, and hybrid)?
5. Can you discuss about the costs for configuration and maintenance involved with your organization's choice of Active Directory deployment model?
6. How does bank business handle integration with other systems and applications across deployment models?
7. How does the scalability of your Active Directory deployment differ between on-premises, cloud, and hybrid models?
8. What backup and disaster recovery strategies do you have in place for your bank Active Directory deployment?
9. How does the choice of deployment model affect the user experience while using Active Directory services in banking industry?

<u>These are sample interview questions:</u>

1. What are the most **important variables** you evaluate when deciding between a hybrid, cloud, or on-premises Active Directory deployment for your bank?

2. How do you determine the **costs and advantages** of each deployment model? What are the primary cost drivers and potential savings?

3. What are the primary **security and compliance considerations** for each model in Ethiopia's banking sector and how do you maintain data security and regulatory compliance?

4. How do you keep **identities, access, and privileges** consistent between on-premises and cloud and hybrid resources and What are the main identity life cycle management methods and tools?
5. How do the various models affect your IT operations and **staffing needs** as well as What impact will this have on your IT team's skills, duties, and responsibilities?

# Reference


(Binduf, A. A.-O. (2018, April). Active directory and related aspects of security. In 2018 21st . Saudi: Saudi Computer Society National Computer Conference (NCC) (pp. 4474-4479). IEEE.).

Ahmad, A. (2019). Empirical analysis on accounting information system usage in banking sector. *Academy of Accounting and Financial Studies Journal, in Jordan.*, 23(5), pp.1-9.).

Ali, S. H. (2022). Evaluating factors contributing to the failure of information system in the banking industry. . *Plos one, 17(3), p.e0265674.*

Active directory and related aspects of security. In 2018 21st. (April, 2018). Saudi: Saudi Computer Society National Computer Conference (NCC) (pp. 4474-4479). IEEE.).

Assefa, S. &. (2018). Determinants influencing cloud computing adoption decisions in small and medium enterprises in Ethiopia. *African Journal of Business Management,, 12(8),* , 457-468.

Banstola, B. (2021). Hybrid Active Directory Integration.

Beynon-Davies, P. ( 2019). Business information systems. . Bloomsbury Publishing.).

Binduf, A. A.-O. (n.d.).

Binduf, A. A.-O. (2018, April). Active directory and related aspects of security. *Saudi Computer Society National Computer Conference* (pp. (pp. 4474-4479)). Saudi: (NCC). IEEE.).

Cybellium. (2023). A Comprehensive Guide To Learn Active Directory.

Dashen Bank partners. (Aug 22, 2022). *IBM to for cloud integration in Ethiopia,,.* Africa's business, economy,www.ceobusinessafrica.com/tag/africa/).

Deb, M. a. (2021). Hybrid cloud: A new paradigm in cloud computing. *Machine Learning Techniques and Analytics for Cloud Security,* , 1-23.

Francis, D. .. (2017). Mastering Active Directory. *Packt Publishing Ltd*.

Francis, D. (2021). Mastering Active Directory: Design, Deploy, and Protect Active Directory Domain Services for Windows Server 2022. . *Packt Publishing Ltd.*

Gillis, W.-C. (2023). Active-Director.

Giuseppe Di Federico, F. B. (2022). Design enterprise cloud identity models with OAuth 2.0 and Azure Active Directory.



Giuseppe Di Federico, F. B. (2022). Design enterprise cloud identity models with OAuth 2.0 and Azure Active Directory.

McDonald, G. P. (2022). Ransomware: Analysing the impact on Windows active directory domain services. p.953.

Ooi, J. P. (2023). The adoption of smart warehouse in Shah Alam: A qualitative study on the decisive factors . *(Doctoral dissertation, UTAR)*.

Rashid, M. A. (2022). Financial information security using hybrid encryption technique on multi-cloud architecture. *Bulletin of Electrical Engineering and Informatics, 11(6),*, pp.3450-3461.

Raza, M. I. (2019). A review on security issues and their impact on hybrid cloud computing environment. . *International Journal of Advanced Computer Science and Applications, 10(3).)*.

Sangwan, S. a. (June 2015). Addressing Security issues for Enterprises Migrating to HYBRID Cloud Computing Mode. *International Journal on Recent and Innovation Trends in Computing and Communication, 3(6),*| , pp.3618-3622.

Subbarao, D. R. (2023). Microsoft Azure active directory for next level authentication to provide a seamless single sign-on experience. *Applied Nanoscience, 13(2)*, 1655-1664.

Tesema, D. (2020). Cloud computing adoption challenge in case of commercial bank of Ethiopia. *International Journal of Development Research, 10(01),*, pp.33562-33565.

Trovato, F. S. (2019). Cloud, co-location, on-premises and hybrid disaster recovery solutions: Pros, cons, and a cost comparison. *Journal of Business Continuity & Emergency Planning, 13(2),*, pp.120-135.

Uddin, M. A. (2020). Cybersecurity hazards and financial system vulnerability: . *a synthesis of literature. Risk Management,, 22(4)*, 239-309.

Zannone, N. Z.-M. (2023). Security Analysis of Azure Active Directory Logs using Machine Learning.