ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar2027

Reducing Vendor Lock-In in Healthcare Cloud Systems Using Hybrid Cloud Storage Architecture

Rujal Patel[1*]; Vidhi Sutaria[2]

[1]Asha M. Tarsadia Institute of Computer Science and Technology, Uka Tarsadia University, Surat, Gujarat, India
[2]Asha M. Tarsadia Institute of Computer Science and Technology, Uka Tarsadia University, Surat, Gujarat, India

Corresponding Author: Rujal Patel[1*]

Publication Date: 2026/04/08

Abstract: The rise of cloud computing has transformed healthcare IT, providing scalable data storage and analysis (through telemedicine services), and offering data analysis for patients' Electronic Health Records (EHRs). While cloud technology brings with it significant advantages, many healthcare organizations are at risk of becoming dependent on a single cloud provider, due to vendor lock-in (where organizations are forced to use only the infrastructure and services offered by one cloud provider to access their healthcare data). Vendor lock-in can create challenges, including limited system interoperability and increased cost and complexity when moving healthcare data from one cloud provider to another. The hybrid approach to cloud storage outlined in this paper provides a solution to reducing vendor lock-in for cloud-based solutions in the healthcare industry. The proposed hybrid approach consists of combining local storage (a private storage environment) with public cloud storage (Amazon S3). The solution uses a lightweight lifecycle management system implemented with Python, to automatically identify archived, inactive records and move them to public cloud storage while also maintaining frequent access records on local storage. With this architecture, hybrid cloud implementing a hybrid storage model for healthcare organizations will allow them greater flexibility for future storage options and an improved ability to manage data throughout its lifecycle by reducing their reliance on one cloud provider.

Keywords: *Vendor Lock-In, Hybrid Cloud, Healthcare Informatics, Cloud Storage, Multi-Cloud Architecture.*

How to Cite: Rujal Patel; Vidhi Sutaria (2026) Reducing Vendor Lock-In in Healthcare Cloud Systems Using Hybrid Cloud Storage Architecture. *International Journal of Innovative Science and Research Technology,* 11(3), 3595-3600. https://doi.org/10.38124/ijisrt/26mar2027

I. INTRODUCTION

Around the world, health care organisations are using Cloud Computing Technologies to help store, manage and transmit electronic health records; support telemedicine services; and help facilitate medical data analytics [18]. With these advantages, it has been easy for many health care facilities to benefit from Cloud Computing Technologies and expand their digital transformations at an accelerated pace.

Unfortunately, while Cloud Computing Technologies provide many benefits, there are many challenges associated with their use. One of the largest challenges facing health care providers today is the challenge of Vendor Lock In [7]. Vendor Lock In refers to a situation in which an organisation relies heavily on one vendor (service provider) of Cloud Computing services. In this case, moving data or applications from one vendor's Cloud services to another vendor's Cloud services is extremely difficult due to proprietary technologies, services that are specific to the vendor's platform, and limitations on transferring data from one vendor to another [6].

The vendor lock-in problem is especially problematic for healthcare systems. These organizations carry a heavy regulatory burden regarding the length of time medical records are to be retained [9]. If a healthcare organization becomes dependent on a single vendor for cloud use, it will likely incur substantial financial costs and technical challenges to migrate its highly sensitive patient data from one vendor to another [25].

To address this factor, this paper proposes that a hybrid cloud storage strategy will use automated processes to classify medical files according to their date of creation and to migrate those files appropriately based on the amount of time that has passed since they were created [27]. By using the hybrid visual file identification method and by automating the life cycles of those files, the hybrid storage strategy will

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar2027

result in improved resource utilization and reduced dependency on a singular cloud vendor.

The proposed storage strategy and the automation scripts that run under this strategy will rely on the use of Python automation scripts and AWS Cloud Services. As a result, the proposed hybrid cloud storage strategy will provide an automated process to monitor the local storage and to upload older files that have been stored locally to the Amazon S3 archive once they exceed the expiration date [15].

The proposed hybrid cloud storage strategy illustrates an alternative to address the cloud vendor lock-in issue by demonstrating how a hybrid cloud storage strategy can help healthcare organizations achieve a balance between their performance, cost efficiency and independence from using any one cloud vendor [22].

II. RELATED WORK

A significant amount of research has been conducted on the issue of vendor lock-in resulting from the use of cloud computing [25]. When companies use significant amounts of resources through one cloud vendor's proprietary service, this forms an attachment/relationship that makes it very challenging to switch vendors or move applications or data [4].

Several studies have highlighted the need for cloud platforms to be interoperable to limit vendor dependency [6]. Solutions that were described include the use of containerization, open standards, and multi-cloud architectures [26].

Healthcare systems are increasingly reliant on cloud computing as a necessary infrastructure; examples of these uses are to house electronic health records for medical professionals and to support telemedicine and perform analytics on healthcare data [8]. While these cloud systems can help healthcare in improving patient care, there are many significant challenges for the healthcare industry that include data privacy, security, and vendor dependency [28].

Hybrid and multi-cloud architectures are new strategies that offer greater flexibility to organizations to limit their reliance on any single cloud provider and increase system resiliency by distributing the workload across multiple platforms [10].

Despite the advances being made in the field, most of the studies published in this area are based on theoretical/guide frameworks and there are few examples that have been published that demonstrate actual hybrid cloud-based strategies for managing healthcare data [15].

➢ *Problem Statement*

Cloud computing is a great way to manage your healthcare data; however, being tied to one cloud provider presents many operational challenges and potential risks. Vendor lock-in limits the flexibility of healthcare organizations and can make migrating their data from one platform to another quite challenging [7].

Healthcare organizations need to be able to store a complete history of their patients medical records, while also making sure that the data is accessible and secure, as well as compliant with the applicable regulations.

This presents a serious problem for healthcare organizations because, if they become completely dependent on a single cloud provider, then they may have to make extensive changes to their physical infrastructure in order to migrate data away from that provider, which can be costly.

As a result of these challenges, healthcare organizations need to look at cloud architectures that offer them the ability to maintain some level of flexibility while still utilizing scalable cloud infrastructure [27].

➢ *Proposed System: Hybrid Cloud Architecture*

The proposed architecture represents a hybrid cloud storage solution by combining the local infrastructure with public cloud storage [27].

- *The Architecture Includes These Three Main Components:*

Local Storage System - The local storage system enables the use of a private cloud environment for the storage of regularly used healthcare data.

Public Cloud Storage - The Amazon S3 storage solution enables the archiving of healthcare data from the cloud.

Data Life Cycle Management Module - The lightweight life cycle management function allows the automatic movement of inactive data from local storage to cloud storage.

This architecture will ensure that health care data that is in use will remain in local storage while older historical records will automatically move to cloud storage. This design provides for effective management of storage space while maintaining redundancy and dependency on one external provider of cloud services [22].

III. SYSTEM ARCHITECTURE

The hybrid cloud architecture proposes that integrating a local storage method with public clouds will enhance and promote a more flexible and efficient way to manage health information, as opposed to relying on a single cloud service provider. The workflow for the proposed hybrid cloud architecture is shown in Figure 1.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar2027

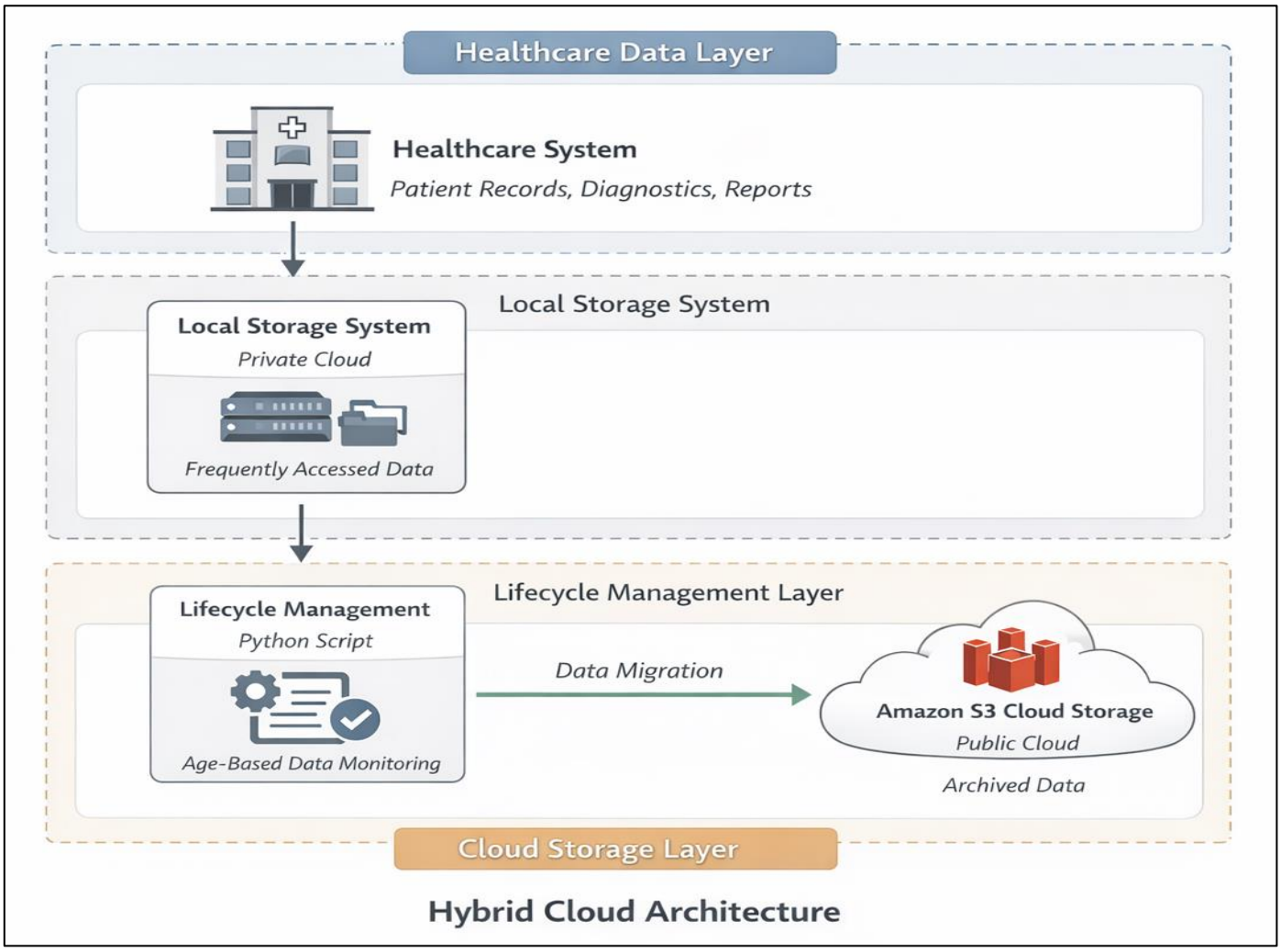

Fig 1 Hybrid Cloud Architecture for Healthcare Data Lifecycle Management.

The architecture is composed of three main components: healthcare data layer (provides access to frequently accessed medical records), life cycle management layer (automation of moving data from local to cloud storage infrastructure), and cloud storage layer (stores less frequently accessed healthcare data).

Healthcare Data Layer - The healthcare data layer is the local storage of frequently accessed medical records, the private cloud for where health information is generated; this layer will also contain newly generated health information (i.e. patient records, diagnostic imaging reports, clinical documentation), providing for improved speed at which healthcare providers can access information needed for patient care.

Data Lifecycle Management Layer - The lifecycle management layer enables the movement of data from local storage to cloud resources. An automation script written in the Python programming language constantly checks the local storage directory to determine how long each file has resided there. If any file has been in the local storage directory for longer than a preset period (e.g., 60 days), that file will automatically be sent to the corresponding cloud storage.

Cloud Storage Layer - The cloud storage layer uses the public cloud resource for long-term storage of archived health records. The architecture of the system utilizes Amazon S3 because of the large amount of data that needs to be saved in the long term (for example, hundreds of thousands of patient records). The use of S3 allows for easy scalability and reliability. All archived records are now saved in one S3 bucket, while the local (on-premise) storage continues to contain the currently-active healthcare records.

IV. IMPLEMENTATION

Using Amazon S3 and Python, a prototype was constructed to demonstrate the proposed hybrid cloud model outline.

Included in the prototype is a lifecycle management program that scans through a directory of local healthcare records. This program checks the age of each file and determines if it should remain in local storage or if it should be archived remotely on the cloud. The workflow of the lifecycle management process is illustrated in Fig. 2

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar2027

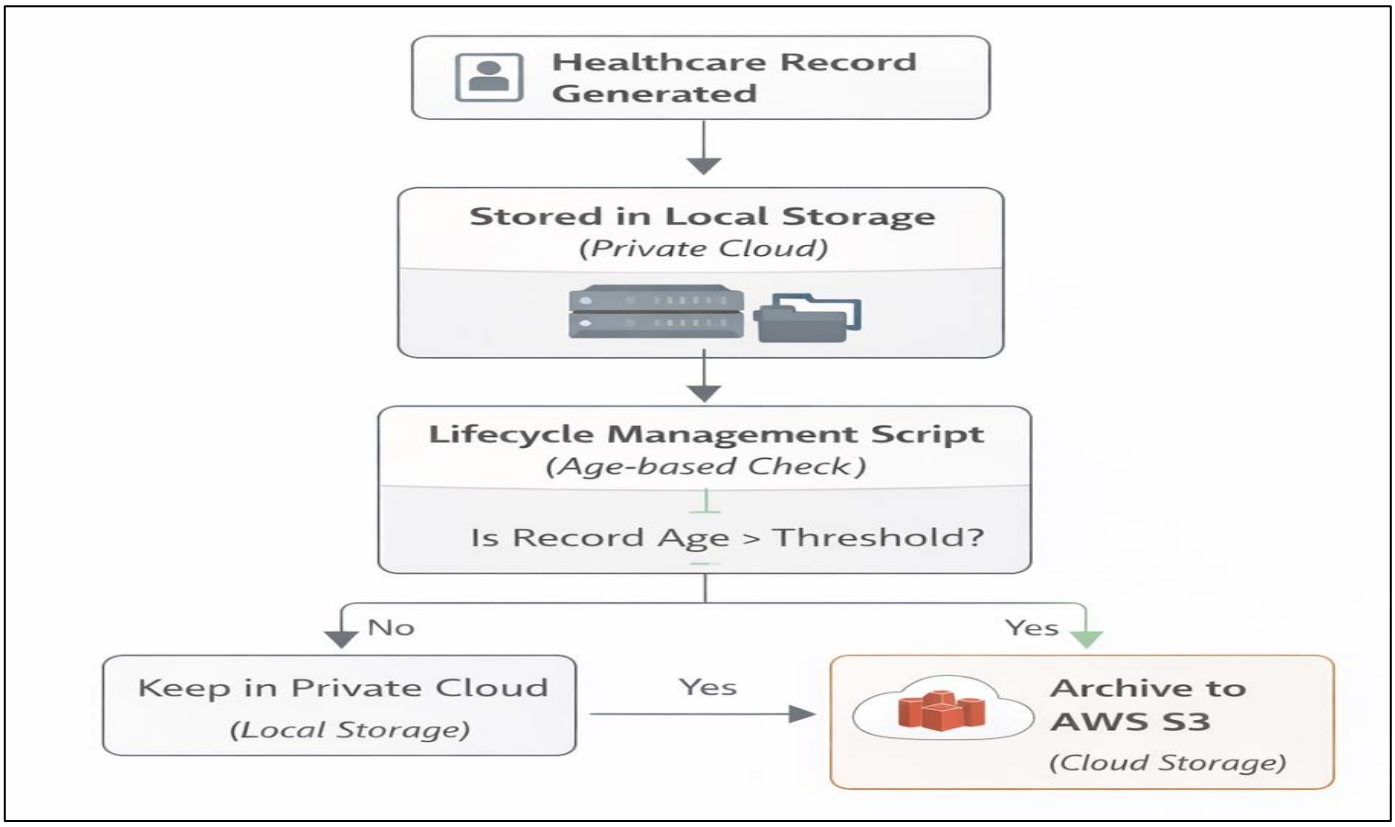

Fig 2 Healthcare Data Lifecycle Workflow for Automated Migration Based on a Configurable Threshold.

The lifecycle management program supports a threshold of 60 days to determine the age of the file and will automatically upload the file to the Amazon S3 bucket if it has aged beyond this threshold. Files that have an active use are retained in local storage.

An example of the implementation of the lifecycle management program using Python to monitor local directories and migrate inactive records automatically can be seen in Fig. 3.

```python
hybrid_storage_manager.py > ...
import os
import time
import boto3

LOCAL_FOLDER = "healthcare_data"
BUCKET_NAME = "healthcare-hybrid-archive-12345"
DAYS_OLD = 60

s3 = boto3.client("s3")
current_time = time.time()

print("🔍 Scanning healthcare records...\n")

for file_name in os.listdir(LOCAL_FOLDER):
    file_path = os.path.join(LOCAL_FOLDER, file_name)

    if os.path.isfile(file_path):
        age_days = (current_time - os.path.getatime(file_path)) / (60 * 60 * 24)

        if age_days > DAYS_OLD:
            s3.upload_file(file_path, BUCKET_NAME, file_name)
            print(f"✅ Uploaded: {file_name}")
        else:
            print(f"⏳ Active file: {file_name}")

🔍 Scanning healthcare records...
✅ Uploaded: patient_001_report.pdf
✅ Uploaded: patient_002_xray.jpg
✅ Uploaded: patient_003_report.pdf
✅ Uploaded: patient_004_report.pdf
✅ Uploaded: patient_005_report.pdf
```

Fig 3 Python-Based Lifecycle Management Script Used to Monitor Healthcare Records and Automatically Migrate Inactive Files to Amazon S3.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar2027

An example of migrated healthcare records being successfully stored in the Amazon S3 bucket is presented in Fig. 4, illustrating that the proposed hybrid cloud model is effective.

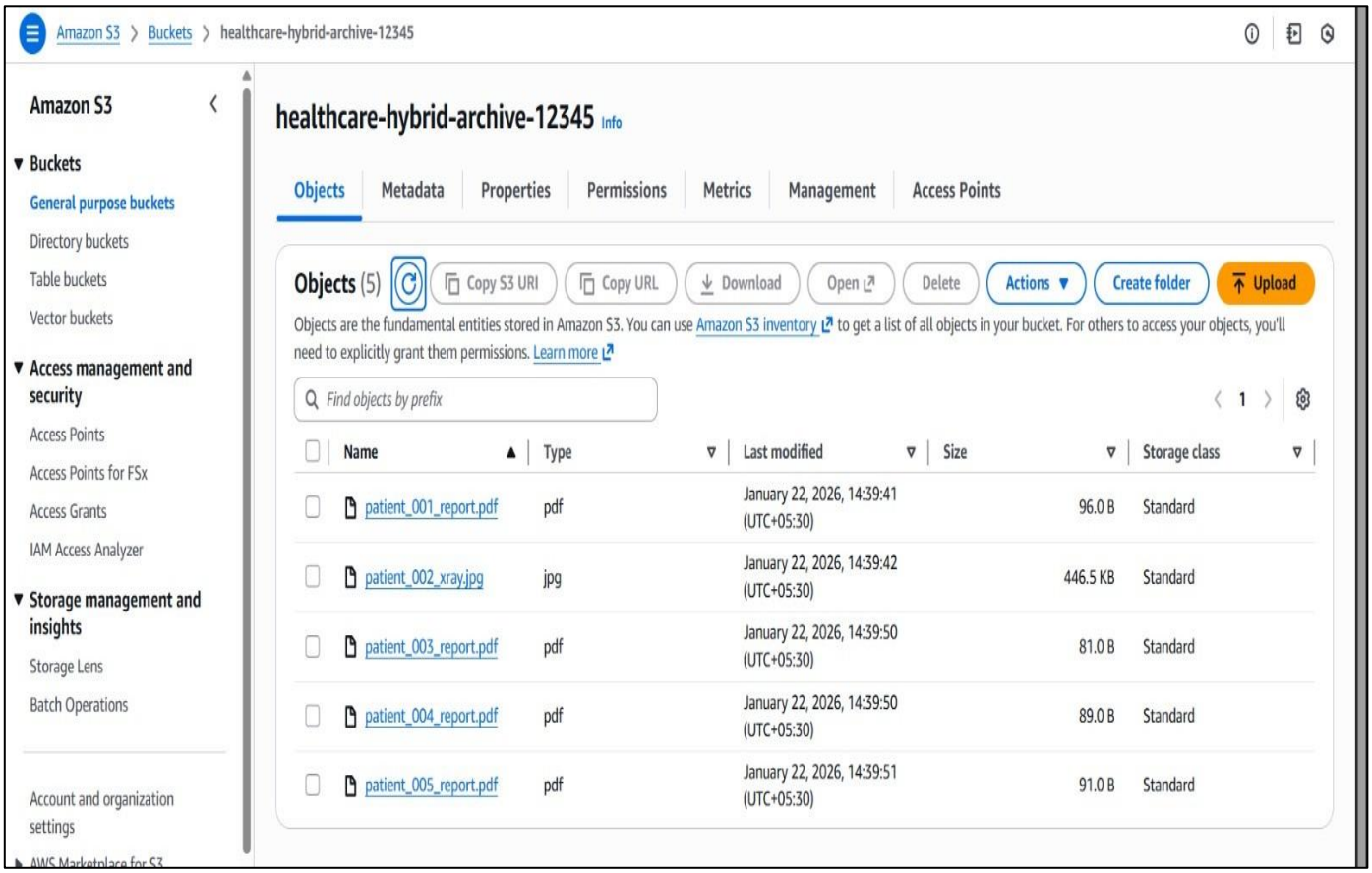

Fig 4 Healthcare Records Stored in the Amazon S3 Bucket After Automated Migration from Local Storage.

This automated process will allow health care organizations to maintain a hybrid storage solution and decrease the amount of manual effort in managing data.

V. RESULTS DISCUSSION AND EXPECTED IMPACT

Healthcare cloud systems will benefit from a number of features and benefits from the proposed hybrid cloud architecture (HCA).

Firstly, this solution reduces vendor lock-in due to local and cloud storage (data will be saved locally for immediate access), giving healthcare organizations control over critical data and expanding their options to use larger, scalable cloud infrastructure [25].

Secondly, automated lifecycle management enhances storage efficiency through the archiving of inactive records to cloud (primary) storage as well as maintaining a record database.

Thirdly, hybrid cloud architectures can enhance resiliency of the systems using redundancy between local and cloud storage. This type of resiliency is an important consideration when implementing a hybrid cloud approach [27].

Currently there are prototypes of hybrid cloud based medical systems, but studies show that there may be significant improvements in flexibility of cloud medical systems using hybrid architectures than currently exist [15].

To evaluate the effectiveness of the proposed hybrid cloud architecture, a conceptual comparison between the traditional cloud system and the hybrid cloud system is shown in Table 1.

Table 1 Comparison Between the Traditional Cloud System and the Proposed Hybrid Cloud System.

Parameter	Traditional Cloud System	Hybrid Cloud System
Vendor Dependency	High	Reduced
Scalability	Limited to Moderate	High
System Flexibility	Low	High
Storage Cost	High	Optimized
Data Management	Manual	Automated

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar2027

VI. CONCLUSION

The subject of the research is vendor lock-in in regards to the use of cloud platforms, more specifically hybrid cloud platforms for healthcare [7].

The proposal consists of a hybrid solution made out of a combination of local storage (hardware) and the usage of public cloud services (e.g., Amazon S3). The proposed hybrid solution has been designed to operate as follows: when records are no longer accessed frequently, they will automatically be archived to the public cloud while still providing local access to frequently accessed healthcare records.

The findings of this research support the idea of hybrid cloud architectures providing lower dependence on only one provider while increasing the flexibility of storage and providing new ways of managing the life cycle of an organization's data [27].

Future directions of research may include approaches to implementing multi-cloud deployments as well as developing more sophisticated frameworks for interoperability between the various pieces of the healthcare cloud environment [30].

➢ *Funding*

The authors received no financial support for the research, authorship, and/or publication of this article.

➢ *Ethics and Consent to Participate*

Not applicable.

REFERENCES

[1]. T. Ismail et al., "Hybrid and Secure E-Health Data Sharing Architecture in Multi-Cloud Environment," in *Proc. Int. Conf. Advanced Intelligent Systems*, 2020.
[2]. H. Zhang et al., "Multi-Cloud Storage Systems: A Survey," *IEEE Access*, vol. 8, pp. 123–145, 2020.
[3]. Y. Li et al., "Kubernetes-Based Container Orchestration for Multi-Cloud Deployments," *Future Generation Computer Systems*, vol. 115, pp. 123–134, 2021.
[4]. S. Chen et al., "Cloud Portability and Vendor Lock-In Mitigation Strategies," *IEEE Transactions on Cloud Computing*, vol. 9, no. 3, pp. 1012–1025, 2021.
[5]. J. Kim et al., "Container-Based Application Portability in Multi-Cloud Environments," in *Proc. IEEE Cloud*, 2021.
[6]. L. Wang et al., "Cloud Interoperability and Vendor Lock-In Prevention Techniques," *Journal of Cloud Computing*, vol. 11, no. 2, 2022.
[7]. P. Kumar and P. Kumar, "Vendor Lock-In Situation and Threats in Cloud Computing," *IJISRT*, vol. 7, no. 9, 2022.
[8]. A. Patel et al., "Secure Healthcare Data Management Using Cloud Computing," *IEEE Access*, vol. 10, pp. 45678–45690, 2022.
[9]. K. Cresswell et al., "Key Challenges and Opportunities for Cloud Technology in Health Care," *JMIR Human Factors*, vol. 9, no. 2, 2022.
[10]. J. Alonso et al., "Understanding Multi-Cloud Native Applications," *Journal of Cloud Computing*, vol. 12, 2023.
[11]. M. Giacomini and A. Ullah, "YASF: A Vendor-Agnostic Framework for Serverless Computing," in *Proc. ICEIS*, 2023.
[12]. P. R. Naidu et al., "Advancements in Multi-Cloud Applications for Enhanced E-Healthcare Services," in *Proc. ICAIIHI*, 2023.
[13]. E. Ok and J. Owen, "Breaking Down Barriers in Cloud Computing," *Cloud Computing Journal*, 2023.
[14]. O. Hope, "Enterprise Multi-Cloud Deployment Models," *IEEE Cloud Computing*, 2023.
[15]. P. Singh et al., "Hybrid Cloud Storage Architecture for Healthcare Systems," *Springer Healthcare Systems*, 2023.
[16]. S. Patel et al., "Multi-Cloud Computing for Healthcare Data Analytics," *Elsevier Computer Networks*, 2023.
[17]. N. Mohammad, "Cloud Computing and Its Impact on IT Infrastructure," *IJCS*, 2024.
[18]. A. Sapkal et al., "Evolution of Cloud Computing," *IRJET*, 2024.
[19]. G. Ayepola and P. Abos, "Vendor Lock-In and Interoperability," *International Journal of Cloud Applications*, 2024.
[20]. A. Hamza, "Impact of Containerization in Reducing Vendor Lock-In," M.S. thesis, 2024.
[21]. A. Alhosban et al., "CVL: A Cloud Vendor Lock-In Prediction Framework," *Mathematics*, vol. 12, no. 3, 2024.
[22]. A. Raheem, "Hybrid and Multi-Cloud Strategies for Enterprise Systems," *IEEE Access*, 2024.
[23]. D. Seth, "Navigating Multi-Cloud Architecture," *Springer*, 2024.
[24]. E. Kamau, "Real-Time Data Synchronization in Multi-Cloud Systems," *Future Internet*, 2024.
[25]. A. Kumar, "Vendor Lock-In Mitigation in Cloud Platforms," *Cloud Systems Journal*, 2024.
[26]. M. Waseem et al., "Containerization in Multi-Cloud Environments," *IEEE Access*, 2024.
[27]. L. Lopez, "Hybrid Cloud Architectures for Healthcare Systems," *Healthcare Informatics Research*, 2024.
[28]. R. Gupta et al., "Hybrid Cloud Security for Healthcare Data Systems," *IEEE Security & Privacy*, 2024.
[29]. A. Rahman et al., "Secure Data Migration in Hybrid Cloud Environments," *Journal of Network Security*, 2024.
[30]. T. Zhou et al., "Interoperable Multi-Cloud Frameworks for Healthcare Systems," *IEEE Access*, 2024.
[31]. A. Amanna and I. Shinde, "Zero-Trust Architecture for Healthcare Cloud Systems," *IEEE Security*, 2025.
[32]. P. Venkiteela, "Vendor-Agnostic Multi-Cloud Integration Framework," *Cloud Computing Advances*, 2025.
[33]. A. A. M. Ghalib, "Cloud Computing: Architectures, Security Paradigms, and Future Directions," *JETIR*, 2025.