

Assessment Cover Sheet

Assessment Title	Thesis Document		
Assessment Type	Uncontrolled	Individual	Not must-pass
Due Date	28 th December 2025	Course Code	IT7099
Course Title	IT Project		
Internal Moderator's Name	Bahruz Mashrequi		
External Examiner's Name			

Instructions:

1. This cover sheet must be completed (section in red below) and attached to your assessment before submission in hard copy/soft copy.
2. The time allowed for this assessment is 8 weeks
3. This assessment carries 30 marks assessing CILO 1, CILO 2 and CILO 4.
4. The materials allowed for use in this assessment are Thesis (Design + Technical) document.
5. The use of generative AI tools is strictly prohibited.
6. References consulted (if any) must be properly acknowledged and cited.
7. The assessment has a total of XXX pages.

Learner ID	202203753	Date Submitted	28/12/2025
Learner Name	Ali AlRashedi		
Programme Code	IT-7099		
Programme Title	IT Project		
Lecturer's Name	Dr.Cyril Anthoni		

By submitting this assessment for marking, I affirm that this assessment is my own work.

Learner Signature

Ali AlRashedi

Do not write beyond this line. For assessor use only.

Assessor's Name	
Marking Date	Marks Obtained

Comments:

*A Cloud Infrastructure using Microsoft Azure in
Managing Secure and Scalable Brain Tumor
Detection System for Hospitals.*

by

Ali AlRashedi

A Thesis Submitted in
(Partial) Fulfillment of the
Requirements for the Degree of

Bachelor of Science
in Information & Communication Technology

at

Bahrain Polytechnic

December 2025

Title

*A Cloud Infrastructure using Microsoft Azure in
Managing Secure and Scalable Brain Tumor
Detection System for Hospitals.*

Copyright

© 2025

Ali AlRashedi

All rights reserved

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgment has been made in the text.

Signature Ali AlRashedi Name Ali AlRashedi Date: 12/11/2025

Approval Signatures

APPROVED FOR THE ICT PROGRAMME

(thesis supervisor), Thesis Supervisor Date

(writing tutor), Technical Writing Tutor Date

Abstract

The implementation of the use of secure and scalable infrastructure within the Microsoft Azure Cloud to enable a healthcare system for the management and processing of confidential medical information. The primary intention is to develop a secure atmosphere within the cloud infrastructure for secure networking, managed access, secure data storage, and stable system operation, taking into account the requirements of healthcare data protection and information security. The system development is designed to handle complex workloads such as data analytics and machine learning, but without making such workloads the key elements of the system.

A systematic approach in infrastructure engineering was used, starting from requirement analysis and cloud architecture design, and progressing to system deployment and setup. The deployed solution brings into place Microsoft Azure Virtual Networks (Azure VNet) along with subnets to separate system components, Network Security Group (NSG) to specify traffic control policies, private endpoints to reduce public access to essential services, and secure storage and database resources for managing patient data. Other security features, including encryption, site monitoring, and Site-to-Site Virtual Private Network (VPN) connectivity, were also deployed to ensure patient confidentiality and prevent unauthorized access.

Keywords: Microsoft Azure, Cloud Infrastructure, Healthcare Systems, Network Security, Data Protection, Network Security Groups, Virtual Private Network, Virtual Networks, Healthcare, Machine Learning.

Acknowledgements

First of all, I would like to acknowledge with gratitude my project supervisor, Dr. Cyril Anthoni, who has been guiding me throughout the semester with his invaluable suggestions and support. His suggestions have played a crucial role in determining the technical direction of this project, thereby improving its overall quality.

Secondly, I would like to thank Bahrain Polytechnic for providing the resources and academic environment to help build this project.

Lastly, I would like to thank my family and friends for their continued encouragement and support throughout my project period. Their patience and encouragement played a crucial role in my successful completion of this project.

Table of Contents

Title	I
Declaration.....	III
Abstract.....	V
Acknowledgements	VI
Table of Contents	VII
List of Figures	XI
List of Tables	XIII
List of Symbols	XIV
List of Abbreviations.....	XV
1. Introduction.....	1
Project Rationale	1
Project Objectives	2
Prior Work	2
Hypothesis	3
Proposed Solution	3
Description of the Report	4
Chapter 2: Background	4
Chapter 3: Design	4
Chapter 4: Implementation.....	4
Chapter 5: Testing	4
Chapter 6: Discussion	5
Chapter 7: Conclusion	5
Chapter 8: References.....	5
Chapter 9: Appendices.....	5
2. Background	6
Introduction	6
Related Theory	6

Used and Considered Technology	7
Related Work & Literature Review	10
Market Research	11
3. Design	13
Requirements and Design	13
UML Diagrams	13
General System Use Case Diagram (Infrastructure View)	14
Use Case Diagram - Manage Cloud Resources	15
Use Case Diagram – Manage Security	16
Customer Perspective Use Case Diagram	17
Activity Diagram – Data Transfer	18
System Architecture	19
Full Azure Topology Diagram (Infrastructure Architecture)	19
Deployment Diagram – Azure Infrastructure Deployment	20
4. Implementation	24
Overview of implementation	24
Azure Network Creation	24
Subnet Deployment	25
Web App Subnet	26
ML Subnet	27
Database Subnet	27
Web App Backend Subnet	27
Management Subnet	27
Development Subnet	28
Security Deployment	28
NSGs	28
Firewall	29
Site-to-Site VPN	33
Storage Implementation	36
Blob Storage	37
Database Implementation	40
Model Deployment	41
Monitoring, Logging & Security Tools	44

Azure Monitor	45
5. Testing	46
Test Plan.....	46
Participants.....	1
Functional Requirements Test Cases and Results	1
Acceptance Test Process and Results	5
Usability Testing Results and Statistics.....	6
6. Discussion, LESPI, and Conclusion	10
System Functionality	10
Accomplished Objectives	10
Project Issues	12
Backup Plan.....	13
Future Plan and Work	14
Synopsis of my experience.....	15
Bahraini Perspectives	15
Legal, Ethical, Social, and Professional Issues	16
Legal Issues	16
Ethical Issues.....	17
Social Issues	17
Professional Issues.....	18
7. Conclusion	19
8. References:.....	20
9. Appendices.....	26
User Manual	26
Purpose and Intended Users.....	26
System Overview for Users	26
Network Access.....	26
Cloud Services Resources.....	28
Monitoring System health.....	30
Limitations on User Interaction.....	31
User Manual Summary	31

System Manual	32
Purpose and Responsibilities.....	32
Network Administration	32
Secure Connectivity Management.....	33
Cloud Compute Resources.....	41
Machine Learning Infrastructure.....	46
Monitoring and Logs	49
System Manual Summary	50
Appendix II: Detailed Design.....	51
Purpose.....	51
Architecture Design.....	51
Network Design.....	51
Site-to-Site VPN Design Requirements.....	53
Cloud Compute Resources Design	54
Data Storage and Database Design.....	55
Appendix IV: Detailed Implementation	57
Setting up the environment	57
Setting up Services	63
Setting up Security.....	68
Configuration scripts	69
Usernames and Passwords:	Error! Bookmark not defined.

List of Figures

Figure 1: Use Case Diagram of Infrastructure.....	14
Figure 2: Use Case Diagram for Managing Cloud Resources	15
Figure 3: Use Case Diagram for Managing Security.....	16
Figure 4: Customer Perspective Use Case Diagram	17
Figure 5: Activity Diagram for Data Transfer	18
Figure 6: Azure Topology Diagram	20
Figure 7: Deployment Diagram for Azure Infrastructure.....	21
Figure 8: Deployment Diagram Azure	21
Figure 9: VNet Creation Summary-1	25
Figure 10: VNet Creation Summary - 2	25
Figure 11: Cloud Brain Tumor Subnets	26
Figure 12: Network Security Groups	29
Figure 13: Firewall Manager	30
Figure 14: Firewall Dashboard	31
Figure 15: Firewall Policy Dashboard.....	32
Figure 16: Firewall Policy	33
Figure 17: VPN Gateways	34
Figure 18: vpngw-cloud dashboard.....	35
Figure 19: vpngw-onprem dashboard.....	36
Figure 20: Storage Account Overview	37
Figure 21: Blob Storage.....	38
Figure 22: Scans Container Blob Storage.....	39
Figure 23: Reports Blob Storage Container.....	40
Figure 24: Database Overview.....	41
Figure 25: ML Container Dashboard	43
Figure 26: Test URL.....	44
Figure 27: Monitor Activity Log.....	45
Figure 28: Bastion Ping to simulated on Premises.....	1
Figure 29: Success Ping from On Premises to Cloud Bastion VM.....	2
Figure 30: Web NSG Inbound and Outbound Security Rules	3
Figure 31: Logs Of Recent Activities on Storage Account	4
Figure 32: Active Database Connection (Development DB)	5
Figure 33: Blob Storage Performance Metrics on Ingress	7
Figure 34: PostgreSQL Database Active Connections.....	8
Figure 35: Blob Storage Performance and Statistics on Ingress, egress, latency, and Request metrics	9
Figure 36: VPNgw-Cloud Connection to on Premises	27
Figure 37: VPNgw- Onprem connection to cloud	28
Figure 38: VMSS Status	29
Figure 39: Virtual Machines Status.....	30
Figure 40: Activity logs.....	31
Figure 41: Network Security group Test server NSG	33
Figure 42: VPN Gateway in Hybrid Connectivity Overview.....	34
Figure 43: Recommended layout to start VPN setup	35
Figure 44: Site-to-Site VPN connection setup -1.....	36

Figure 45: Site-to-Site VPN connection setup -1.1.....	37
Figure 46: Site-to-Site VPN connection setup -2.....	38
Figure 47: Site-to-Site VPN connection setup -2.1.....	39
Figure 48: Site-to-Site VPN connection setup -3.....	40
Figure 49: Site-to-Site VPN connection setup -3.1.....	41
Figure 50: On Premises VM deployment Complete	43
Figure 51: VMSS Dashboard.....	44
Figure 52: Test Server Deployment Summary -1	45
Figure 53: Test Server Deployment Summary -2	46
Figure 54: Health of ML model	47
Figure 55: ML model Test Data.....	48
Figure 56: ML Model Test Data Outcome	49
Figure 57: Azure Cloud Design	51
Figure 58: Subnet layout.....	52
Figure 59: Site-to-Site VPN Tunnel Diagram	54
Figure 60: Compute and Processing Diagram	55
Figure 61: Storage and DB Architecture	56
Figure 62: Resource Group Creation.....	57
Figure 63: Resource groups Tab	58
Figure 64: Vnet Creation pt-1	59
Figure 65: Vnet Creation pt-2	59
Figure 66: Vnet Creation pt-3	60
Figure 67: Vnet Creation pt-4.....	60
Figure 68: Vnet Creation pt-5	61
Figure 69: Vnet Creation pt-6.....	61
Figure 70: Installation of Azure CLI.....	62
Figure 71: Powershell Azure CLI Installation version.....	63
Figure 72: Web-DB configuration	63
Figure 73: Web DB Configuration Summary.....	64
Figure 74: Summary Deployment.....	64
Figure 75: Storage Account creation.....	65
Figure 76: Deploy Storage Account Success.....	66
Figure 77: Pushing ML model to Azure.....	67
Figure 78: Web deployed	68

List of Tables

Table 1: List of Abbreviations	XVI
Table 2: Comparison of Technologies Considered.....	9
Table 3: Technologies Used	10
Table 4: Participants in Test Cases	1
Table 5: Functional Requirements Test Cases.....	2
Table 6: Acceptance Test Process Results.....	6
Table 7: Project Issues and Solution	13
Table 8: IP Scheme	52

List of Symbols

No table of Symbols entries found.

This Project does not contain any Symbols.

List of Abbreviations

Abbreviation	Full Form
VM	Virtual Machine
VMSS	Virtual Machine Scale Set
VNet	Virtual Network
IP	Internet Protocol
VPN	Virtual Private Network
Site-to-Site VPN	Site-to-Site Virtual Private Network
Vpngw	VPN GateWay
IPSec	Internet Protocol Security
NSG	Network Security Group
NACL	Network Access Control List
ELB	Elastic Load Balancing
S3	Simple Storage Service
AWS	Amazon Web Services
SQL	Structured Query Language
Azure VNet	Microsoft Azure Virtual Network
WAF	Web Application Firewall
APA	American Psychological Association
DNS	Domain Name System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VPC	Virtual Private Cloud
IAM	Identity and Access Management
MFA	Multi-Factor Authentication
API	Application Programming Interface
OS	Operating System
CPU	Central Processing Unit
CLI	Command Line Interface
RAM	Random Access Memory
DB	Database
ML	Machine Learning
AI	Artificial Intelligence
MRI	Magnetic Resonance Imaging
VPN Gateway	Virtual Private Network Gateway
ISO	International Organization for Standardization
ISO 27001	Information Security Management Standard ISO 27001

HIPAA	Health Insurance Portability and Accountability Act
GDPR	General Data Protection Regulation
PDPL	Personal Data Protection Law (Bahrain)
GCC	Gulf Cooperation Council
GIS	Geographic Information System
SLA	Service Level Agreement
KPI	Key Performance Indicator
ARM	Azure Resource Manager
CI/CD	Continuous Integration and Continuous Deployment
CIA Triad	Confidentiality, Integrity, Availability Triad
DevOps	Development Operations
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
SaaS	Software as a Service

Table 1: List of Abbreviations

1. Introduction

An Azure-based platform to support machine learning for identifying brain tumors based on MRI inputs. It is essential to have an efficient, scalable, and trustworthy technology solution in real-world healthcare applications, given that early diagnostic analysis is, in many instances, made more difficult due to the expertise needed for visual analysis. It is necessary for MRI uploading, inference, and result storage to have such a project create a hybrid platform for cloud computing by leaning on features such as encrypted uploading, isolation, private routing, availability, or continuous monitoring. Other aspects in reporting on this project shall cover its context, method, implementation, analysis, and conclusion.

Project Rationale

The proposed work aims at creating and demonstrating the secure cloud architecture for an automatic system for the detection of brain tumors. When the images are analyzed by the radiologists, differences are observed, thereby leading to risks and delays in healthcare. Even though cloud technology provides faster processing, scalability, and efficiency, health platforms are still struggling to implement architectures, scalability, and security requirements. According to (Oh et al., 2015), health platforms, considering the implementation of cloud architecture, require handling issues related to privacy and security along with appropriate quality attributes.

The value of reliable computing environments has been highlighted in studies on medical AI. There are already cases of Azure-based systems being used for medical imaging, with cloud computing making it easy to set up models and manage data. Specifically, Azure Machine Learning was used to “train and deploy state-of-the-art machine learning models for cancer classification” (Hamed, El, Tarek Abd El-Hafeez, & Omar, 2024). The general use of cloud computing is also examined in a research study, and it verifies the role of cloud computing in improving the health sector, as trends in research are on improving capability, workflow, and efficiency (Ali, Shrestha, Soar, and Wamba, 2018).

Project Objectives

The aim is to offer a secure, scalable, and organized cloud infrastructure so as to allow fast processing of the MRI scans.

- Architect an Azure infrastructure with VNets, subnets, NSGs, WAF, load balancers, Azure App service, and VM Scale Sets.
- Utilize computational capabilities to manage tasks related to model training and inference.
- Apply Azure Monitor to gain operational visibility.
- Support integration of the machine learning process with front-end interfaces of radiologists.
- Ensure data security and privacy practices are appropriate for the healthcare industry.

Limitations and Concerns

- The cost and availability of GPU-enabled VMs may be limited.
- Because MRI files are so large, this creates storage and transfer issues.
- Scaling a balance between demand and financial limitations.

Prior Work

Cloud systems have been used in the past to support health applications, but still, design and security are significant concerns, as shown by numerous studies. According to (Oh et al., 2015), there is the need for well-designed platforms organized in well-structured components, focusing on “interface, business services, cloud SaaS, quality attributes, privacy, and security.” This is in line with the focus on the design of Azure and secure deployment.

Azure has been used within actual diagnostic tasks in studies involving cancer imaging, proving the capability of Azure. “The use of ‘Azure Machine Learning ...to train and deploy’ machine learning models showcases the benefit of cloud computing in improving medical imaging applications,” as mentioned in (Hamed, El, Tarek Abd El-Hafeez, & Omar, 2024).

The analysis of cloud computing in the health sector by (Ali, Shrestha, Soar, & Wamba, 2018) draws attention to the significance of cloud systems, stating that the topic "provides a systematic review of scholarly articles on cloud computing in the healthcare sector." This gives emphasis to the significance of organized, accurate, and safe systems.

Although these studies provide useful insights, they also point to certain weaknesses, as they are model-centric, rather than considering the overall operation environment. There are few studies on comprehensive architecture for cloud computing, ranging from networking and security mechanisms to scalability and integration. This new industry fills the gap by developing an Azure infrastructure tailored only for the deployment of clinical artificial intelligence.

Hypothesis

The hypothesis states that with an optimized architecture on the Azure Cloud, performance, reliability, and security will improve for the automated tumor detection process in the human brain. This will be achieved through the utilization of features such as secured VNets and components of Azure ML, among other features. The process will handle MRI images faster compared to the former manual processes. Also, the cloud setup will be able to handle high traffic and provide privacy and continuous operation of the system.

The system's success, controlled access, robust security, and low diagnostic times serve as evidence of the successful operation of the system.

Proposed Solution

The functional core of the system for the brain tumor detection system is implemented on Microsoft Azure. The deployment involves virtual networks, NSGs, WAF, VM Scale Sets, storage accounts, and monitoring tools. Machine learning is linked with the front-end interface used by radiologists and doctors, and this takes place on Azure virtual machines. The monitoring of the system can be done through Azure Monitor.

Providing strong data privacy for their patients, robust performance under high usage, and dependable MRI processing are all guaranteed by this architecture. It also provides a deployment model for hospitals.

Description of the Report

Chapter 2: Background

This chapter will cover the concepts and technology being used in the proposed project, including cloud computing, Azure infrastructure, virtualization, and machine learning concepts in medical images. The chapter will also compare other platforms, studies, and the gaps this proposed endeavor will fill, as well as conducting research on the current state of the market for medical imaging systems and how the proposed system will improve those systems.

Chapter 3: Design

The topic of this chapter is system requirements, architecture, and designs. The proposed deployment of Azure components, networking, and security tools is examined and analyzed.

Chapter 4: Implementation

This chapter will detail how this system is developed, a step-by-step guide based on the Project Implementation phase, highlighting key aspects of implementation along with guidance.

Chapter 5: Testing

The chapter describes the test plan cases, processes, and environments used in validating system behavior. Performance, security, stress, participants involved, and functional tests are used, and their outcomes and findings are shown.

Chapter 6: Discussion

In this chapter, the outcome of the tests and their relation to the objectives will be assessed. This chapter will discuss achievements, limitations, hindrances, Bahraini perspectives, lessons learned during development, future work, and LESPI reflection.

Chapter 7: Conclusion

In this chapter, the findings obtained from this research will be summarized, and the hypothesis will be addressed.

Chapter 8: References

In this report, all the sources used are referenced in APA format.

Chapter 9: Appendices

The following chapter contains more details, including diagrams, configurations, and screenshots.

2. Background

Introduction

This section contributes to the creation of a safe cloud environment for brain tumor detection and analysis system in healthcare. The project uses cloud to support MRI image data processing, machine learning computation, and connectivity to hospital networks using secure and controlled connectivity. To form the basis for development, this chapter introduces the concepts, technology, and previous research needed to develop an infrastructure that can support medical procedures that are delicate and sensitive within a secure network environment. It also identifies factors related to network security, data transfer, and other issues encountered when shifting patient data from within hospital networks to cloud technology. The remaining parts and subtopics include analyses related to cloud network concepts, machine-learning environments, and various technologies within respective cloud services, with studies and opportunities within the proposed solution development.

Related Theory

The infrastructure for the brain tumor detection solution must adhere to the principles of cloud networking, computing, secure data management, and hybrid communication. Medical imaging applications produce large quantities of private information, requiring segmentation, encrypted communications, and strict information security in cloud environments. Zero-trust model, virtual network isolation, or encrypted routes could be some theoretic foundations for managing secure interactions among parts in such a multi-subnet environment. High availability and redundancy principles have extreme significance, given their relevance in medical applications, impacting many diagnostic capabilities. Most healthcare setups have some regional, on-site infrastructure, requiring secure communication with cloud services via VPN tunnels, thereby validating claims for hybrid cloud theory.

Regulations such PDPL, GDPR, or HIPAA apply pressure on infrastructure planning with stipulations on encryption, controlled route utilization, data retention boundaries, audit trail support, or restricted administrative interfaces (Rezk, Alshathri, Sayed, Hemdan, & El-

Behery, 2025). Such principles are most readily applicable to topology planning for their own project with their VNets, restricted traffic routes, secure MRI data transport, or separate administrative communication.

Used and Considered Technology

Microsoft Azure is utilized for project infrastructure, with full functionality aimed at managing MRI scans, model inference, and associated storage in an appropriate, secure, and scalable fashion. Azure Virtual Networking is divided into subnetworks representing web, backend, machine-learning, database, and management layers for faster communication. Site-to-Site VPN connectivity to Azure encrypts communication to the network, creating secure MRI scan upload communications free from any internet presence, thereby maintaining absolute safety with appropriate enablement for Azure connectivity. Inbound/outbound communication filtering is enabled via Azure Firewall, Web Application Firewall, protecting entry points to applications in general. Business-continuity-based ML Compute endpoint communication functions in restrictively controlled ‘ML Subnet’s, maintaining absolute isolation via NSG firewalls, resulting in flow acceptances from specially allowed services.

Furthermore, Azure Blob storage maintains MRI scan storage with encryption to support ‘lifecycle management’ for storing long-term MRI scan retention, with an allowed PostgreSQL server in ‘database subnetwork’s to maintain ‘replication for meta data, inference result’s for inferred safety. Utilization for asynchronous communication between ‘ML Computations enabled layers to ‘AKS backend Cluster’s enhances overall ‘Dependability’s for high ‘system usage’s via ‘Azure Queueing Storage’s, which decreased latency with multiple executions in Azure’s profound grandeur for ensuring world wide applications usages’ absolute safety’s optimal characterization’s with Azure. Azure ‘Monitor’s, ‘Log Analytics’s support overall ‘end to end’s ‘event visualizations from home to Azure’s appropriate networks via ‘compliance, performance, Analytics’, ‘Cost’s in utterly optimistic ‘frontiers’ via banding defined computational feasibility’s (Hannan, 2025).

This project requires that its cloud setup supports safe data storage for MRI images, secure machine learning operations, and safe connectivity with the facilities within the healthcare institutions. Effective network segmentation, controlled traffic flow, secure data transfer procedures, and role-based network administration must also receive highest priority in its core framework since medical patient data must flow from behind its on-premise network to its cloud environment while avoiding connection with any internet traffic. The primary aim in assessing various clouds, therefore, rests on their ability to support the load balancing features, VPNs, firewalls, subnets, security features, and virtual networks required within its medical setup.

Case studies on Azure, AWS, and Google Cloud are also conducted prior to choosing a platform. This evaluation weighs features including private network types, firewalls, hybrid network connectivity capabilities, and how each cloud platform handles routing and isolation controls. Such features directly influence data transfer security in MRI communications, isolation between inference models and public access, and restricting admin control within the cloud platform.

Cloud Platform	Infrastructure Capabilities	Strengths for Infrastructure Design	Infrastructure Limitations
Microsoft Azure (Selected Platform)	VNets, Subnets, NSGs, Azure Firewall, WAF, Bastion, Site-to-Site VPN, Load Balancers, PostgreSQL, Blob Storage	Feature-rich VPN gateway, Azure Firewall for management of inbound and outbound traffic, Bastion for secure admin access, comprehensive isolation capabilities using subnet tiering, seamless integration with ML and DB subnets, and strong compliance for healthcare environments.	Firewalls and Bastions can add to the costs, while latencies are region-dependent, and certain complex routes may require additional configuration.
Amazon Web Services (Considered)	VPC, Subnets, Security Groups, NACLs, Direct Connect, VPN Gateway, ELB, S3, IAM	Worldwide strength, advanced Direct Connect for on-premises connectivity, very extensive router and subnetting features, and flexibly configurable VPC design.	Infrastructure costs can add up fast, availability of Direct Connect can vary widely by region, and interactions between NACL+ and SG are complex.

Google Cloud Platform (Considered)	VPC, Subnets, Firewall Rules, Cloud Router, Cloud VPN, Load Balancing, Cloud Storage	Easy to handle global VPC model; VPN and routing are efficient; internal network has strong performance capabilities; suits analytics-heavy workloads.	simpler networking capabilities than those provided by AWS/Azure; smaller geographical reach; fewer healthcare implementations within the GCC
------------------------------------	--------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------

Table 2: Comparison of Technologies Considered

After reviewing various alternatives, Azure has proved to be most suited to serve its infrastructure requirements. While AWS has extensive global reach capabilities and VPC network customization options, Google Cloud provides efficient internal routing capabilities and simplified global VPC topology. Still, Azure has shown more cohesive and seamless support for its hybrid connectivity, firewalls, and subnet isolation capabilities. The most important reason for preferring Azure is that its infrastructure support services, including Azure Firewall, Bastion, Azure Network Security Groups, and Azure Site-to-Site VPNs, integrate well into Azure's Virtual Network services. As such, the network for the hospital, MRI data storage, ML computation machines, and database servers can all reside within very securely isolated subnets that are better adapted to medical informatics applications.

Technology	Definition/Purpose
Azure Virtual Network (VNet)	A private network that hosts all the subnets. Provides isolation for web, backend, ML, DB, dev, and management layers.
Azure Firewall	Protect virtual network from common attacks such as SQL injection attacks by examining each packet of traffic before it reaches the web interface.
Network Security Groups (NSGs)	Enforce subnet-level traffic policies to limit traffic to allowed ports in order to prevent internal workload exposures. These groups apply to all of the subnets.
Site-to-Site VPN	An encrypted tunnel connecting the hospital network to Azure for transmitting the MRI scans securely without revealing the internal infrastructure. Such a network connection helps in accommodating the hybrid connectivity need of healthcare infrastructure.

Azure App Service (Web App)	Hosts the doctor-facing web portal for uploading the MRI scans and viewing the results of machine learning algorithms.
Application Gateway	Handles incoming traffic, provides SSL termination, and ties in the web application firewall for controlled access to the web tier.
Azure Kubernetes Service (AKS)	Handles backend activities for tasks such as queue processing, in addition to infer requests for routing.
Azure Storage Queue	Handles the storing of the MRI inference jobs being submitted by the web back-end for the purpose of processing.
Azure Blob Storage	Stores the raw images of the MRI scans and the output of the machine learning algorithms in files that support encryption and scalable storage of images.
Azure ML Compute Endpoint	Runs the ML model and returns segmentation predictions. Processes MRI images uploaded via the backend components.
Azure Bastion	Offers safe admin access to virtual machines without exposing public IP information for maintenance activities in the virtual network (VNet).
Azure Monitor	Tracks logs, metrics, alerts, and resource utilization information to offer insights into the health of Machine Learning Endpoints, DB load, and the network.
Azure Database for PostgreSQL (Primary Server)	Stores metadata information, the details of the MRI jobs performed in the application, the logs of events that occur in the application, etc.
PostgreSQL Read Replica	Improves redundancy and reads but reduces the burden on the main server; commonly used for analysis purposes.
Virtual Machine	Used for testing and simulating actual services used
Recovery Services	Offers backup capabilities for databases like PostgreSQL and provides support for disaster recoveries in terms of the VM platform

Table 3: Technologies Used

Related Work & Literature Review

Most studies on brain tumor detection systems are geared towards algorithmic correctness, with less emphasis on the underlying infrastructure for real-world implementation, although studies point out the importance of deep learning in improving classification rates, based on previous research. Studies discuss networked security, such as encrypted data transfer for MRI, yet rarely provide enough information about complete cloud architectures (Ahamed et al., 2023). While studies have yet to provide concrete information regarding real-world applications incorporating network security concepts like encryption, subnet isolation, routing, and network connection, studies have also highlighted importance in having private deep learning networks in medical imaging applications (Rezk, Alshathri, Sayed, Hemdan, & El-Behery, 2025). Studies have also discussed many AI applications having unreliable environments, especially concerning network management, fault-tolerance, and network surveillance (Netshamutshedzi, Netshikweta, Ndogmo, & Obagbuwa, 2025).

Infrastructure gaps in readiness, security, and resilience have also been common in the literature. By incorporating an AKS-based backend, secure Blob Storage, private PostgreSQL connectivity, hybrid connectivity via VPN, monitor pipelines, and Azure with full network segmentation, such limitations have now been overcome in the project under development. According to (Akmalbek Bobomirzaevich Abdusalomov, Mukhriddin Mukhiddinov, & Taeg Keun Whangbo, 2023), such an infrastructure-based paradigm aligns with what healthcare settings require in their practice, beyond what has been expressed in prototypes in the literature.

Market Research

Owing to increasing demand for MRI, pressure on Radiological Departments, and the need to maintain tightened Data Protection Regulations, there's no shortage of adoption of Cloud-based AI-capable imaging solutions in the healthcare industry. With Bahrain encouraging integrated digital healthcare platforms, cloud-ready data flow, and cloud-based data security, regional efforts for Gulf countries on national Digital Health Initiatives clearly depict an immense shift towards secure Cloud-supported infrastructures (Government of Bahrain, 2016). Hence, for Medical Imaging Solutions, there are several

competing platforms in this growing market, each with their inherent strengths and weaknesses. With GIS-based HIPAA-compliant architectures and built-in AI inference, AWS Health imaging ensures efficient, bulk image storage capacity with faster retrievals (AWS Health Imaging, 2025). But to obtain Hybrid Connect with PDPL, an absolutely necessary factor for any healthcare facility, AWS Health imaging itself needs substantial new programming. Though QMENTA, a dedicated neuroimaging platform, features highly advanced MRI analysis tools with impressive biomarkers, optimized MRI, there's no complete network management with QMENTA, with no complete customization too (QMENTA, 2025).

By offering in-built Site to Site VPN, Private Endpoints, Encrypted Storage, Network Segmentation, and Monitoring in one particular environment specifically aimed for ‘Regulated Data’, Microsoft Azure offers a more complete infrastructure support for healthcare applications in comparison to these competing platforms. Azure did gain the highest marks in overall legal, technical, operational feasibility analysis in its feasibility analysis project in regards to its secure architectures with broader Compliances, thereby safely reinforcing such finding. Azure reduces Hardware Costs, thereby Total Cost, deteriorating in prolonged years with minimized operating costs, in sync with the overall transformation in Gulf Region’s healthcare systems, according to a complete cost analysis on feasibility for project plan analysis (PR Newswire, 2025). Azure remains the most appropriate platform for obtaining scalable, secure, and most Compliant Brain Tumor Detection Health Infrastructure, taking into consideration these market realities.

3. Design

Requirements and Design

This section describes the architecture of the cloud infrastructure for the brain tumor detection system and defines the interactions between various system components in the Microsoft Azure ecosystem. The rationale behind this section includes ensuring the project requirements discussed in the earlier chapters are reframed in this section in the form of a system architecture based in the cloud infrastructure. Moreover, system requirements are met through the combined usage of various Microsoft Azure system components.

Various diagrams are utilized in the process of arranging the design. The use case diagram provides information about the key actors and how they can be supported through cloud services. The activity diagram describes the internal process flow and starts from the transfer of data from the MRI system and continues from machine learning processing up to the application retrieval from the database. The deployment diagram provides information about the position of each resource being utilized in the Microsoft Azure structure in the virtual network. The cloud topology diagram provides information regarding the overall structure.

The following sections describe in more detail the various diagrams and how they are relevant in the context of the operational functionality of this system. These descriptions include information about the transfer, processing, storing, and retrieving of the data from the MRI machines over the secure network using Microsoft Azure.

UML Diagrams

General System Use Case Diagram (Infrastructure View)

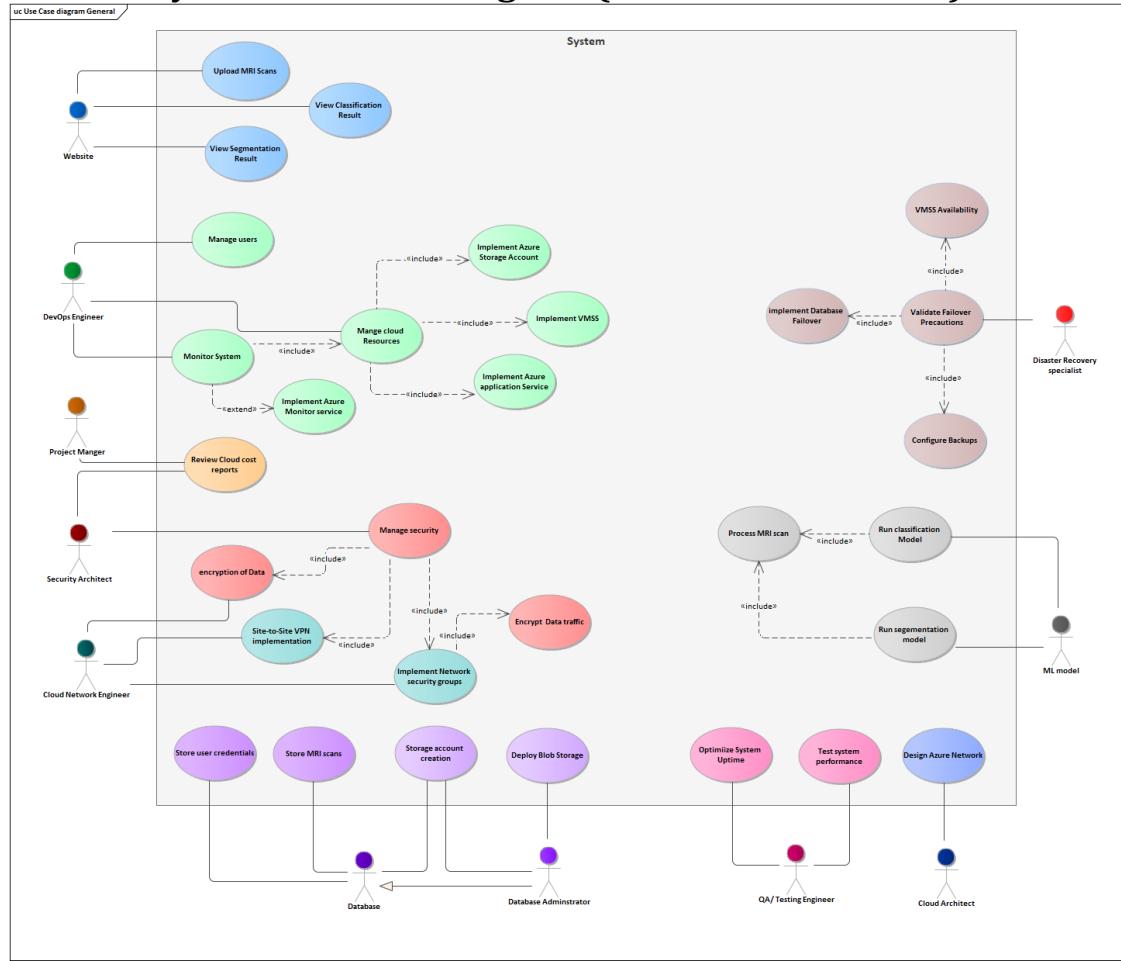


Figure 1: Use Case Diagram of Infrastructure

Figure 1 illustrates how engineers, security architects, monitoring solutions, and machine learning services interact within the cloud environment, giving a global perspective on infrastructural tasks. It is important in that it enables one to understand distinctions between application-layer functions and infrastructural tasks, including provision for resources, VPN management, NSG rules, operations within VMSS, logs, and failover checks. Its role in the project is to designate infrastructural functionality supporting safe data manipulation, data storage, model execution, and MRI upload. In massive medical ML applications, there must be distinct lines between cloud engineers, network security, DevOps, and disaster recovery experts, making this image important in that it addresses this requirement. In earlier stages of cloud infrastructural design, Microsoft recommends

making use of this kind of mapping to design cloud infrastructural solutions, especially for medical applications that need very strict compliance standards (Microsoft, 2025).

Use Case Diagram - Manage Cloud Resources

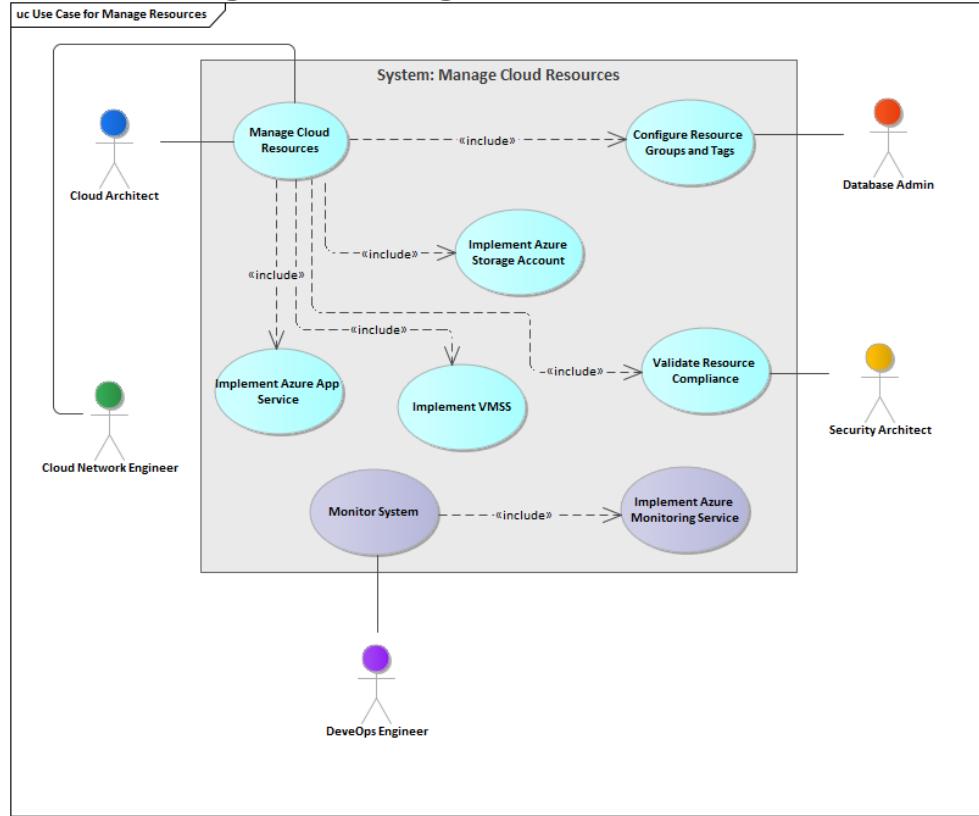


Figure 2: Use Case Diagram for Managing Cloud Resources

The use case diagram for Cloud Resource Management identifies various working processes within providing and maintaining Azure infrastructural resources, including Azure compute services, Virtual Machine Scale Sets, Storage Layers, and resources managed by other organizations for Azure-specific compliances. It also has its usefulness in identifying the roles and responsibilities within respective infrastructural teams for assigning resources to various subnets within the entire system's computational setup. It also intends to prove how various Azure infrastructural resources are created, managed, and tracked for maintaining a scaled-out and steadily performing setup within various applications' working lifespans to support Azure standard recommendations on cloud deployment. This project also uses distinct resource management disciplines that are

essentially required to support ML workloads within ensuring secure Azure infrastructural environments. Moreover, this approach has its highest linkages to concepts within Azure Cloud Adoption Frameworks with its focus on disciplined Azure resources allocation to support long-run enterprise clouds on Azure setup recommendations provided by Microsoft (Microsoft, 2025).

Use Case Diagram - Manage Security

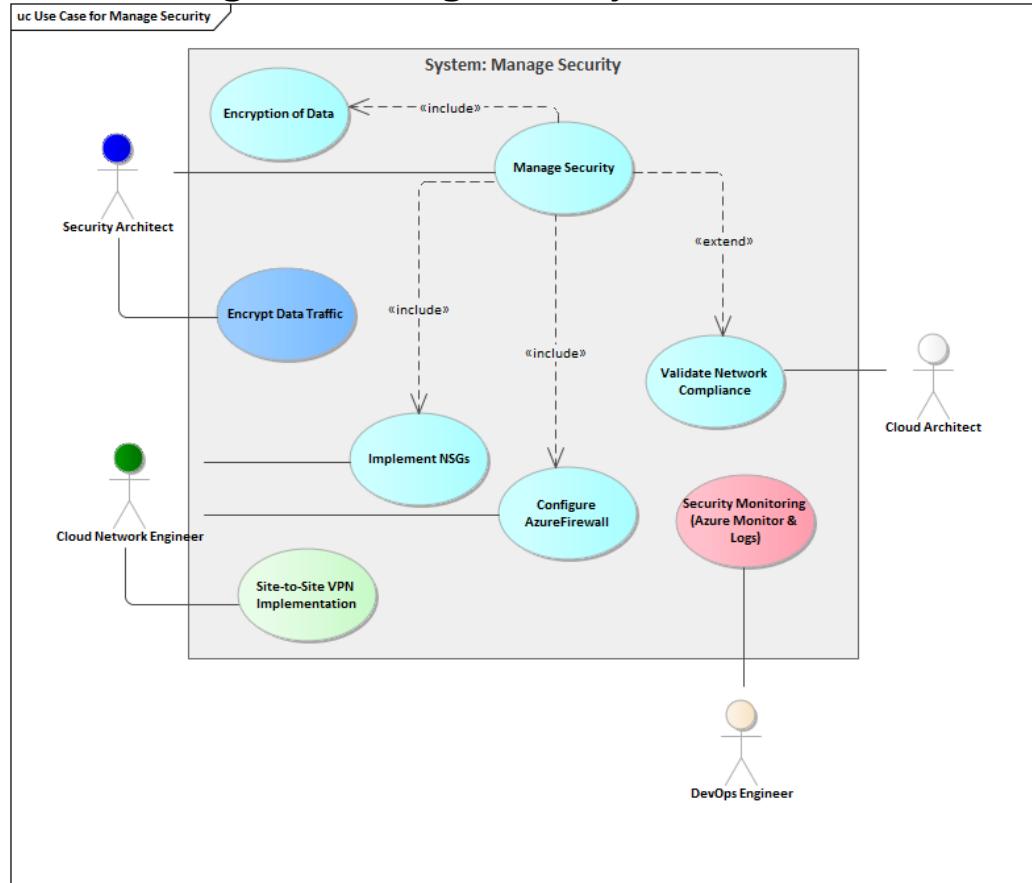


Figure 3: Use Case Diagram for Managing Security.

The Manage Security diagram illustrates the security infrastructural procedures required to ensure data protection for MRI and adherence to medical standards. It is relevant to discuss as it addresses basic steps for network segmentation, VPN connectivity implementation, encryption enforcement, implementation of firewalls and NSG rules, and reliance on Azure's security capabilities to ensure monitoring of system operations. The aim of this project is to identify a methodical ordering approach to ensure security procedures are implemented in totality for ensuring protection pertaining to CIA Triad – confidentiality,

integrity, and availability –of the entire system. This diagram has been selected to prove that secure architectural design on various tiers is essential for environments where protected data needs to be isolated for monitoring. This meets Azure's security benchmark standards for protected procedures to ensure data security for workloads storing delicate medical data (Microsoft, 2025).

Customer Perspective Use Case Diagram

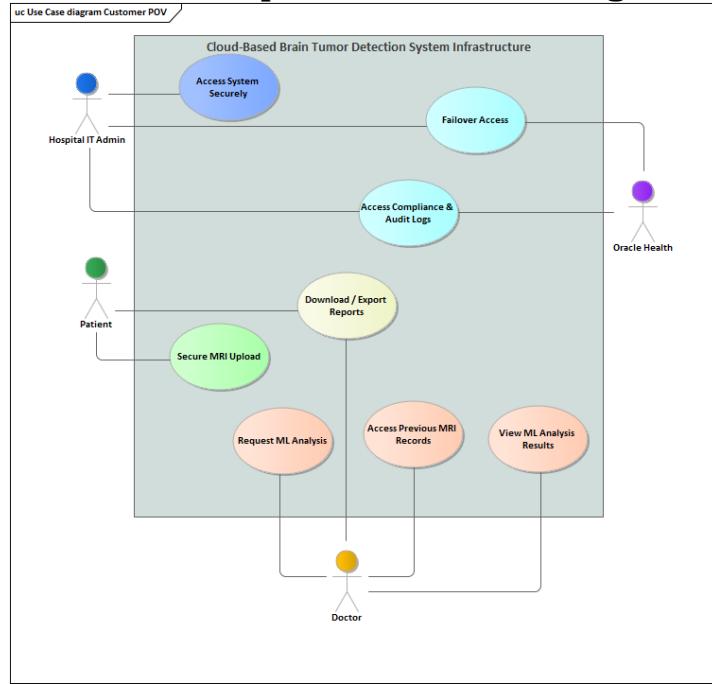


Figure 4: Customer Perspective Use Case Diagram

The customer-oriented use case diagram illustrates how front-end clinical functionality within the patient care environment, including secure MRI image upload, inferencing, access to historical scan data, and system availability during outages, can and does work according to the provided infrastructure. It is important for its ability to link directly from patient care services to encrypted VPN, app gateway filtration, ML compute reliability, or database redundancy, illustrating its work to ensure overall system reliability and patient care functionality within clinical environments by keeping client-level needs on track with technology. The purpose of this diagram is to effectively illustrate the need for proper and secure foundations within patient care capabilities, as is thoroughly validated within cloud computing in healthcare recommendations each year (Microsoft, 2025).

Activity Diagram – Data Transfer

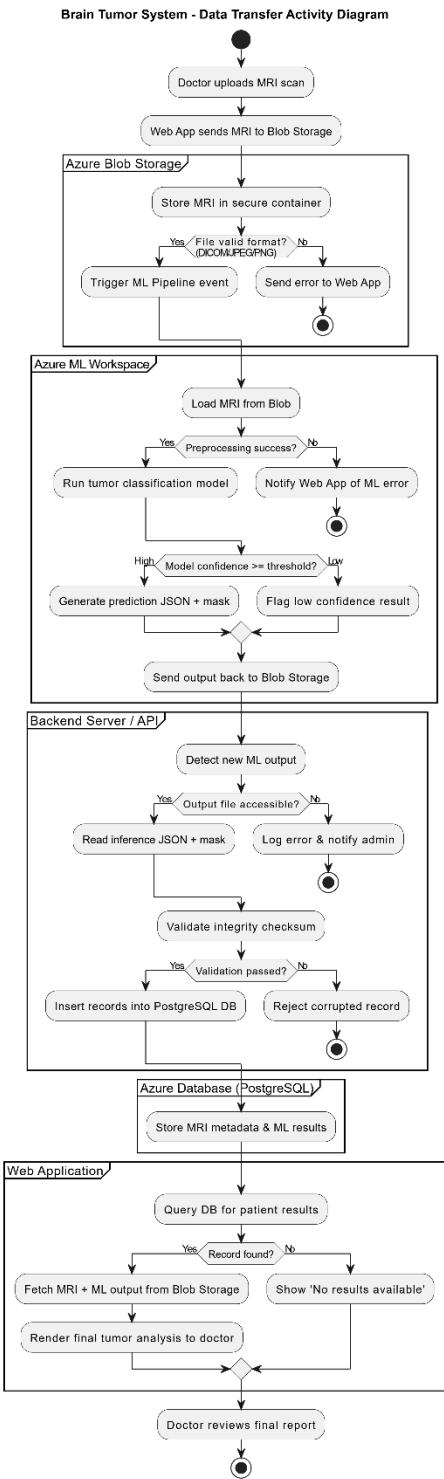


Figure 5: Activity Diagram for Data Transfer

Figure 5 describes the process in the brain-tumor system from the time the clinician uploads the image until the final report is reviewed. The process in the diagram describes how the image is transmitted through the secure web application to the secure object storage in Azure Blob Storage. The process further describes how the image data is processed from the Azure Machine Learning (ML) workspace and how the result received from the classification process is stored in the JSON and mask files. The result can only be stored in the database after being validated by the back-end system before being inserted. This process in the system's conditional logic describes the system's reaction in cases where there are incorrectly formatted files uploaded, failure in the preprocessing stage, failure in the confidence level reached during modeling, or failure in integrity testing of the result obtained from the pipeline process in the system. This process provides assurance to clinicians working with this system that each and every image from the MRI scans goes through secure pipelines that check if the image has passed through proper formatting protocols before being displayed in the clinical interface. This process in the system further underpins the tight connection of clinical workflows and secure protocols developed in the Microsoft cloud system regarding processing images through secure object repositories in Microsoft's Azure (Microsoft 2022; Microsoft 2025; Microsoft 2025).

System Architecture

Full Azure Topology Diagram (Infrastructure Architecture)

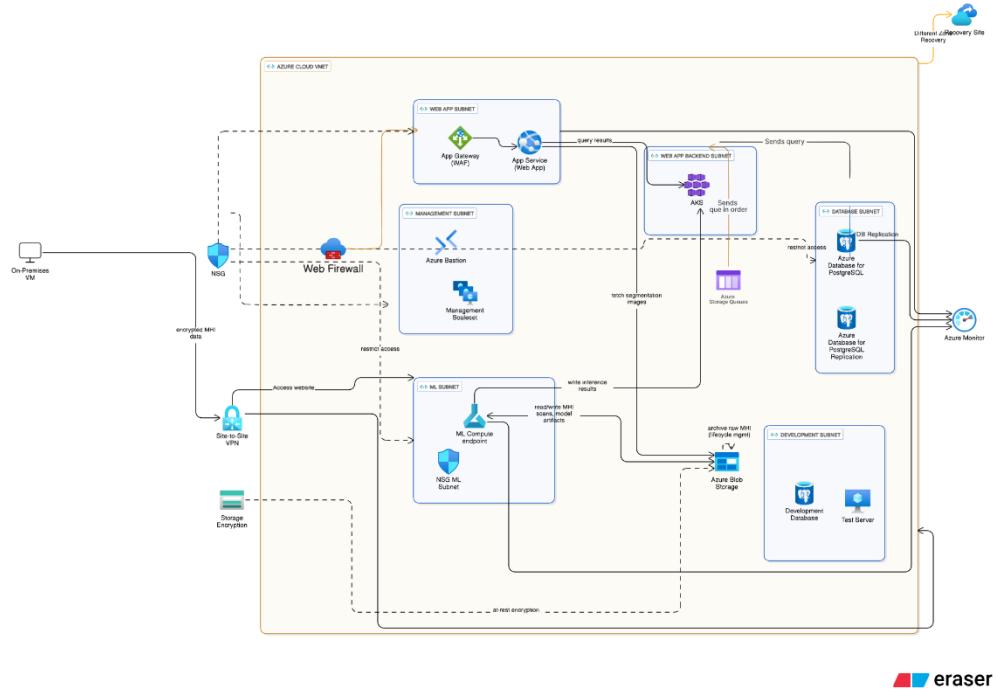


Figure 6: Azure Topology Diagram

The Azure topology diagram with additional details. This diagram illustrates the entire end-to-end infrastructural design, including subnet segregation, VPN tunnels, firewalls, interactions between ML compute services, Blob Storage data flow, AKS processing, database replication, monitoring streams, and disaster recovery capabilities. This is important since it offers a platform where various infrastructural elements and their communication patterns are integrated into one technical platform for implementation, verification, debugging, or suitability check for various infrastructural solutions. The aim of this diagram is to act as the definitive infrastructural representation for the entire system, illustrating how various services work together to ensure safe data processing from MRI sources and successful ML computation execution. This particular diagram was selected since it reflects Microsoft's usual infrastructural architectural patterns for healthcare systems in regulated environments to exhibit well-segmented resources, encrypted data transfer, firm perimeters, and multi-zone resiliency (Microsoft, 2025).

Deployment Diagram – Azure Infrastructure Deployment

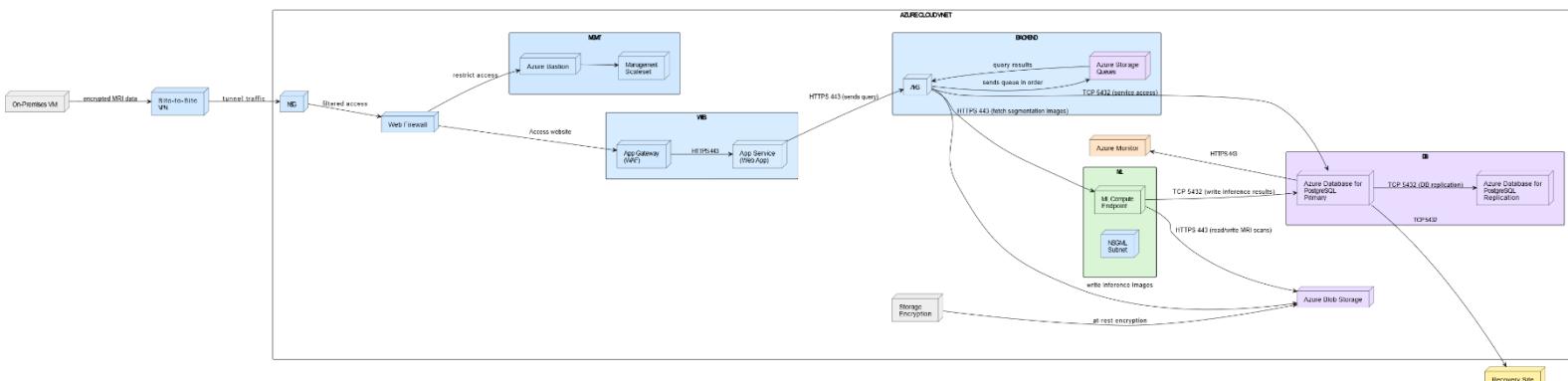


Figure 7: Deployment Diagram for Azure Infrastructure

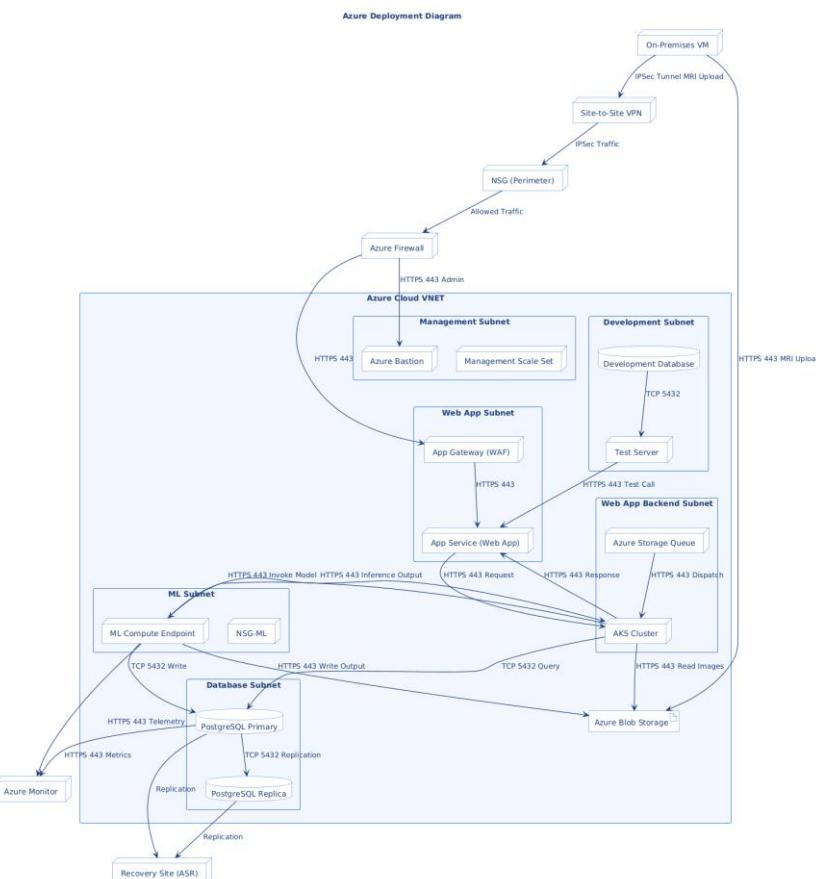


Figure 8: Deployment Diagram Azure

The deployment diagram represents the robust cloud infrastructure utilized for secured magnetic resonance imaging (MRI) data ingestion, machine learning inference tasks, application hosting, and management services in the Microsoft Azure environment. The deployment design incorporates a tiered approach to a zero-trust network architecture to

guarantee the safety of the sensitive healthcare information throughout the processing phases. Communication between the on-premises infrastructure and the Azure services takes place through the encrypted site-to-site IPSec VPN tunnel. The uploading of the MRI information from the on-premises environment travels through the perimeter Network Security Group for screening before reaching the Azure Firewall. This processes extremely restrictive incoming and outgoing rules in the Azure Firewall to allow the highest levels of authorized communications channels in the form of administration via the Azure Bastion service and the web services.

The Azure Cloud Virtual Network (VNET) is segmented into different isolated subnets that add to the overall security, manageability, and compliance of healthcare-related data processing. The Management Subnet holds the Azure Bastion service and the management scale set, offering controlled admin access to the virtual machines without putting them on the public Internet. The Application Gateway service running in the Web App Subnet delivers the Web Application Firewall service capability in addition to the App Service function acting as the secured entry point for all interactions. The application back end exists in the Web App Backend Subnet where the application workflow runs in the AKS cluster and interacts with the Azure Storage Queue to handle the application async tasks.

Machine learning tasks are isolated inside the ML Subnet. This includes the ML Compute Endpoint and the Network Security Group for Machine Learning. Communication between the AKS cluster and the machine learning function happens securely over HTTPS. Additionally, the machine learning endpoint provides inference results for analysis. Isolating the machine learning subnet helps minimize the attack surface and also allows for the allocation of dedicated resources for compute-intensive tasks. Finally, the Database Subnet houses the PostgreSQL primary and secondary databases. These databases hold both transactional information and inference results. Data from the primary database replicates to the secondary on TCP port 5432.

The Development Subnet offers a strictly segregated space for validating applications, database interactions, and backend processes without affecting the processes in the

production environment. The Development Subnet contains a dev database & test server that communicate solely via allowed internal paths. These measures promote operational segregation, prevent the risk of unintentional exposure of the data, and allow for continuous development. Azure Blob Storage is the repository for the MRI files, the segmentation results, & image-related artifacts. The system also allows for the upload of the MRIs from the on-prem site for output to the ML point & image downloads from the AKS environment. Azure Monitor also provides operational observability. This is achieved by collecting telemetry data from the machine learning endpoint, database services, and the rest of the system. The functionality of monitoring the system helps in the early detection of anomalies, optimization of performance, and the healthcare operational requirements for the regulation of the system. Azure Site Recovery provides business continuity. This happens by replicating the database instances and important metadata to a targeted region for recovery.

In conclusion, the deployment architecture showcases a strong, secure, and scalable design optimized for the processing of sensitive MRI images to support machine learning-powered diagnosis. The deployment architecture comprises high availability, the use of encryption for communications, a zero trust approach to segmentation, in addition to the utilization of separate dev and prod environments. All of the subsystems in the deployment architecture combine in the cloud to deliver a solution to the healthcare industry.

4. Implementation

This chapter outlines the cloud architecture developed for the Brain Tumor Detection and Analysis System. The system development is the result of translating the approved architecture of Azure into a working system that enables safe and remote access to the system, machine learning computation, database functionality, and system administration. The designed architecture integrates Microsoft Azure services to accomplish system isolation and security through a multi-layered network architecture.

Overview of implementation

The process of implementation begins with the creation of an Azure Virtual Network tailored to hold all resources for the project. Subnets are then created to organize various workloads, such as web-based access, processing, machine learning computation, data storage in databases, administration, and development. Network Security Groups are implemented on the subnets to manage traffic flow based on least privilege access. The implementation process also does not include Azure Machine Learning, databases, or virtual machines until the network infrastructure has been set up.

Azure Network Creation

The boundary of the private network for the project is demarcated by a single Azure Virtual Network called Brain Tumor-VNet. The VNet is assigned an address space called 10.0.0.0/16, which provides ample room not only for current subnets but also for future growth. All critical service instances operate inside the VNet to enable private communication without direct exposure to the public internet.

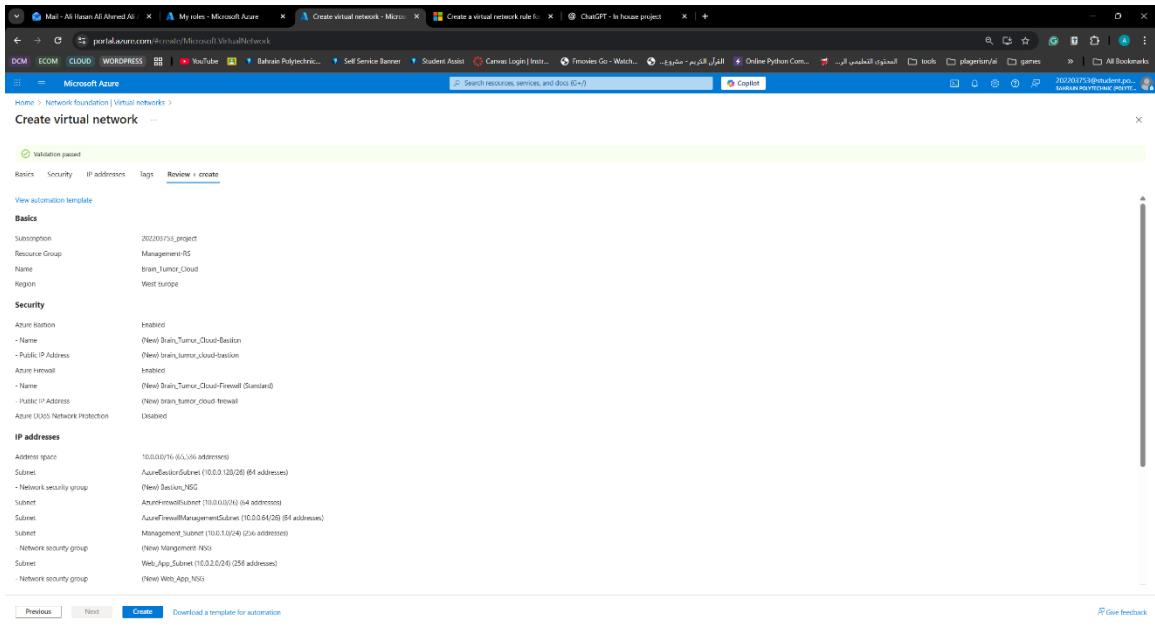


Figure 9: VNet Creation Summary-1

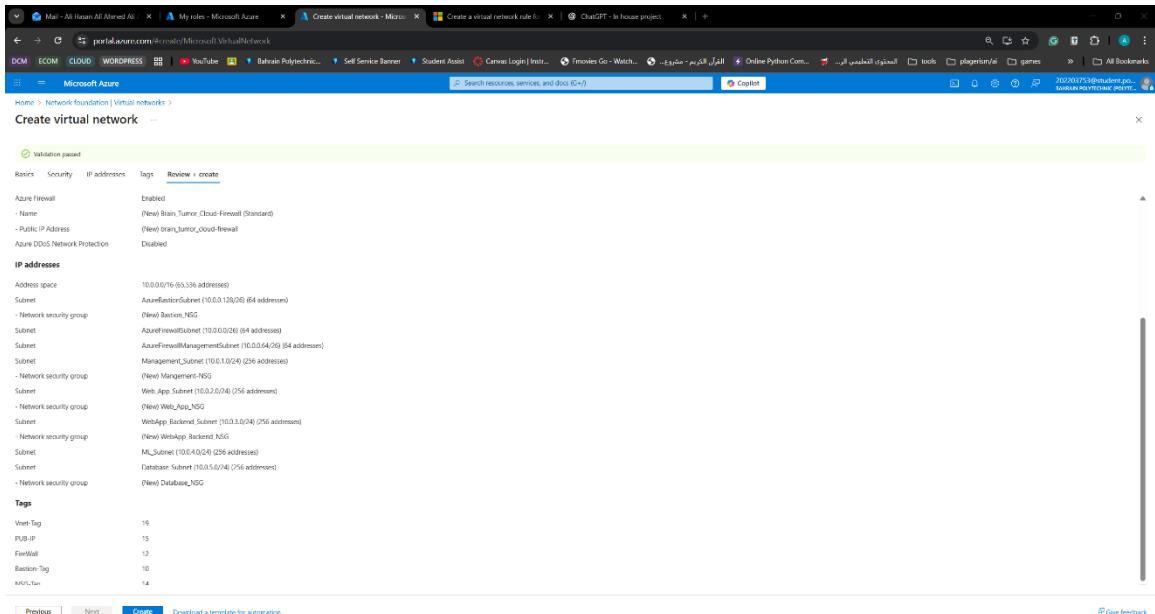


Figure 10: VNet Creation Summary - 2

Subnet Deployment

Multiple subnets were used in the virtual network to create the logical division of workloads. In support of the routing and definition of the security rules, a /24 IP address range was assigned to each subnet to avoid overlapping. This mechanism creates a barrier

for lateral movements for the different services in case there are security issues. Each subnet is also linked to a Network Security Group that defines the allowed inbound and outbound traffic.

The screenshot shows the Microsoft Azure portal interface for managing subnets in a virtual network. The left sidebar navigation menu is visible, with 'Subnets' selected under the 'Virtual network' category. The main content area displays a table of subnets:

Name	IPv4	IPv6	Available IPs	Delegated to	Security group
AzureFirewallManagementSubnet	10.0.0.64/26	-	59	-	-
AzureFirewallSubnet	10.0.0.0/26	-	59	-	-
Web_App_Subnet	10.0.2.0/24	-	249	-	Web
ML_Subnet	10.0.4.0/24	-	251	-	-
Management_Subnet	10.0.1.0/24	-	249	-	Management
Database_Subnet	10.0.5.0/24	-	251	Microsoft....	Data
Development	10.0.6.0/24	-	250	-	-
AzureBastionSubnet	10.0.0.128/26	-	57	-	-
WebApp_Backend_Subnet	10.0.3.0/24	-	251	Microsoft....	Web
GatewaySubnet	10.0.255.0/27	-	availability ...	-	-

Figure 11: Cloud Brain Tumor Subnets

Web App Subnet

The front-end web application was hosted inside the Web App Subnet, which has the address range of 10.0.1.0/24. This subnet is responsible for all communications that are user-facing and is basically the entry point into the system. It only allows traffic to the

necessary web services in the inbound direction and to backend services in the outbound direction. There are no databases or machine learning services exposed to this subnet.

ML Subnet

The resources for Azure Machine Learning were deployed inside the Machine Learning Subnet, and it had a range of 10.0.2.0/24. The ML workspace had a name of ML-space, and it was allocated to a resource group called ML-RS. The Machine Learning Subnet prevents public access and communicates only with approved backend and database services. This is important because it protects sensitive medical images that result from model inference.

Database Subnet

The database subnet was set up using the IP address range 10.0.3.0/24. This subnet does not allow public access but only accepts input messages from the backend subnet and the ML subnet. This setup helps the subnet adhere to the regulations required in the healthcare industry regarding protecting data.

Web App Backend Subnet

The Backend Subnet, which is demarcated by IP addresses 10.0.4.0/24, was created to house application logic and APIs. The Backend Subnet acts as a bridge between the web interface, machine learning components, and database machines. The traffic policy prevents communication from passing through certain internal ports, which ensures that there is a clean separation between the presentation and processing layers.

Management Subnet

The Management Subnet, which has an IP address of 10.0.5.0/24, was established to ensure administrative access, monitoring, and management. The management subnet contains management virtual machines and secure access servers, and there are no application workloads running in this subnet. Additionally, for security purposes, administrative access is restricted to authorized personnel.

Development Subnet

For testing and development, the Development Subnet has been built with the IP address range of 10.0.6.0/24. This testing and development infrastructure allows for controlled development and testing with the maintainability of production services.

Security Deployment

While deploying Azure, the aspect of security was regarded as a basic necessity. The architecture designed incorporating Azure has a defense-in-depth strategy, which entails the use of network segregation, management of traffic, and secure connectivity. Instead of relying on a solitary method to enhance security, a multitier strategy has been used to reduce attack surfaces to counter possible threats. The architecture secures sensitive medical information, machine learning processes, as well as the cloud-hosted application services.

To avoid undesired communication between system components, access control was mandated at the network level via subnet isolation and routing controls. Internal resources were protected from Internet access as connectivity between local environments and Azure resources had been secured without exposing them to the general Internet space. All these factors combined ensured that no external system visibility is achieved and internal system movement is limited.

NSGs

Network Security Groups were established and assigned to each subnet to manage the incoming and outgoing traffic. The rules were developed based on the purpose or function of each subnet, following the least privilege principle. The Web App subnet only allowed incoming web traffic on authorized ports, while the other subnets allowed incoming traffic only from authorized sources within the network. The Database subnet denied all incoming internet traffic and allowed access from the backend and ML subnets. The use of default deny rules prevented unwanted communications.

Network foundation | Network security groups

You are viewing a new version of Browse experience. Click here to access the old experience.

Name	Associated with	Resource Group	Location	Subscription
basicNsgBrain_Tumor_Cloud-nic01	0 subnets, 2 ne...	Management-RS	West Europe	202203753_prc
Bastion_NSG	0 subnets, 0 ne...	Management-RS	West Europe	202203753_prc
Database_NSG	1 subnets, 0 ne...	Management-RS	West Europe	202203753_prc
Mangement-NSG	1 subnets, 0 ne...	Management-RS	West Europe	202203753_prc
Onprem-nsg	0 subnets, 1 ne...	Management-RS	West Europe	202203753_prc
OnPrem-VM1NSG	0 subnets, 1 ne...	Management-RS	West Europe	202203753_prc
Test-Server-nsg	0 subnets, 1 ne...	Management-RS	West Europe	202203753_prc
Web_App_NSG	1 subnets, 0 ne...	Management-RS	West Europe	202203753_prc
WebApp_BACK_NSG	1 subnets, 0 ne...	Management-RS	West Europe	202203753_prc

Figure 12: Network Security Groups

Firewall

Azure Firewall is used as a central network security tool that is responsible for scanning and filtering traffic between subnets and external networks. The Azure Firewall is also responsible for application and network-level policies that block unauthorized access, malicious traffic, and common attack patterns. All Internet traffic that is outbound and originates from internal subnets is forwarded to Azure Firewall, allowing for monitoring and policy application.

The screenshot shows the Microsoft Azure Firewall Manager interface. The left sidebar has a tree view with 'Overview' expanded, showing 'Firewall Manager' selected. Under 'Firewall Manager', 'Azure Firewalls' is selected, which is highlighted with a grey background. Other options include 'Azure Firewall Policies', 'WAF + DDoS', 'Secure your resources', 'Related services', and 'Help'. The main content area displays a table with one row of data. The table columns are 'Name', 'Type', 'Resource Group', 'Location', and 'Subscription'. The single row shows 'Name' as 'BrainTumor-FW', 'Type' as 'Firewall', 'Resource Group' as 'Management-RS', 'Location' as 'West Europe', and 'Subscription' as '202203753_project'. There are filters at the top of the table: 'Subscription equals 202203753_project', 'Resource Group equals all', 'Location equals all', and a '+' button for adding filters. Below the table, there is a message: 'Showing 1 - 1 of 1. Display count: 200'. At the bottom right, there is a 'Give feedback' link.

Figure 13: Firewall Manager

BrainTumor-FW

Overview

Resource group (new) : Management-BS
Location : West Europe
Subscription (new) : 20203735-project
Subscription ID : d846e32f-5a7-4479-be7e-4501eb554495
Virtual network : Brain_Tumor_Cloud
Firewall policy : BrainTumor-FW-Policy
Provisioning state : Succeeded

SKU : Basic (change)
Subnet : AzureFirewallSubnet
Public IP : 10.0.0.4
Private IP : 10.0.0.4
Management subnet : AzureFirewallManagementSubnet
Management public IP : 10.0.0.4
Private IP Range : Managed by Firewall Policy
Route Server (preview) : Add

Firewall policy

Visit Azure Firewall Manager at the link below to edit the Firewall Policy on this firewall.

Policy BrainTumor-FW-Policy (change)

Auto-learn IP Prefixes : Disabled

Rules

DNAT rules	0 rules in 0 collections
Network rules	1 rule in 1 collection
Application rules	0 rules in 0 collections

Threat intelligence

Mode : Alert

TLS inspection

Status : Not supported with basic policy

IDPS

Mode : Not supported with basic policy

Figure 14: Firewall Dashboard

The screenshot shows the Microsoft Azure Firewall Policy dashboard for the policy named "BrainTumor-FW-Policy".

Essentials:

- Resource group: Management-RS
- Location: West Europe
- Subscription: 202203753 project (d844632f-0a17-4479-be7e-4503eb554495)
- Provisioning state: Succeeded
- Tags: Tags (edit), Add tags

Policy inspection:

- Premium
- Not supported with basic policy
- IDPS mode: Premium
- Not supported with basic policy

Policy analytics:

- Policy limits:
 - 1 Rules
 - 1 Unique source/destination: 20,000 Max
 - 0 IP groups: 600 Max
- Rules with multiple IP addresses: Your rules are all good.
- Rules with low utilization: ?
- Static analysis: ?

Navigation:

- Overview
- Activity log
- Access control (IAM)
- Tags
- Resource visualizer
- Management
 - Draft + Deployment (preview)
- Rules
 - Rule collections
 - DNAT rules
 - Network rules
 - Application rules
- Settings
- Monitoring
- Automation
- Help

Search: Search resources, services, and docs (G+)

Feedback: Is That Signature Dangerous To My Network? How can my firewall stop that threat? +1

User Information: 202203753@student.po... BAHRAIN POLYTECHNIC (POLYTE...

Figure 15: Firewall Policy Dashboard

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes tabs for 'My roles', 'BrainTumor...', 'Compute i...', 'frontend...', 'Oracle He...', 'FastAPI - S...', and 'Relaunch to update'. Below the navigation bar are various service icons: GOOGLE AI, DCM, ECOM, CLOUD, WORDPRESS, YouTube, Bahrain Polytechnic..., Self Service Banner, and All Bookmarks. The main title is 'BrainTumor-FW-Policy | Rule collections'. The left sidebar has sections for Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Management (Draft + Deployment (preview)), Rules (selected), Rule collections (selected), DNAT rules, Network rules, Application rules, Settings, Monitoring, Automation, and Help. A message at the bottom left says 'Add or remove favorites by pressing Ctrl+Shift+F'. The right pane displays a table of rule collections:

Name	Type	Priority	Rules	Inherited from
Demo-Rules	Rule collection group	100	1	...
Allow-Internal	Network rule collection	200	1	...

Figure 16: Firewall Policy

Site-to-Site VPN

In order to create a secure and encrypted communication channel between the Azure Virtual Network and the hospital network, a Site-to-Site VPN solution was established. This VPN solution uses IPsec/IKE encryption techniques to ensure the confidentiality and integrity of the patient data sent to the cloud infrastructure. This VPN connectivity would allow trusted systems at the on-premises network to be able to connect to the cloud without risking exposure to the public Internet.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes tabs for 'My roles', 'Hybrid connectivity', 'Compute', 'frontend', 'Oracle', 'FastAPI', and 'Relaunch to update'. Below the navigation bar, there are several quick access links: GOOGLE AI, DCM, ECOM, CLOUD, WORDPRESS, YouTube, Bahrain Polytechnic..., Self Service Banner, and All Bookmarks. The main title is 'Hybrid connectivity | VPN gateways'. The left sidebar has a 'Search' bar and sections for Overview, ExpressRoute, VPN gateway (selected), Set up VPN Gateway, VPN gateways (selected), VPN connections, Local network gateways, and Virtual WAN. The main content area shows a table of VPN gateways:

Name	Resource type	Virtual network	Gateway type	Resource Group
vpngw-cloud	Microsoft.Network	Brain_Tumor_Cloud	Vpn	Management-RS
vpngw-onprem	Microsoft.Network	OnPrem-Sim-VNet	Vpn	Management-RS

At the bottom, it says 'Showing 1 - 2 of 2. Display count: 200'. There are also 'Add or remove favorites by pressing Ctrl+Shift+F' and 'Give feedback' buttons.

Figure 17: VPN Gateways

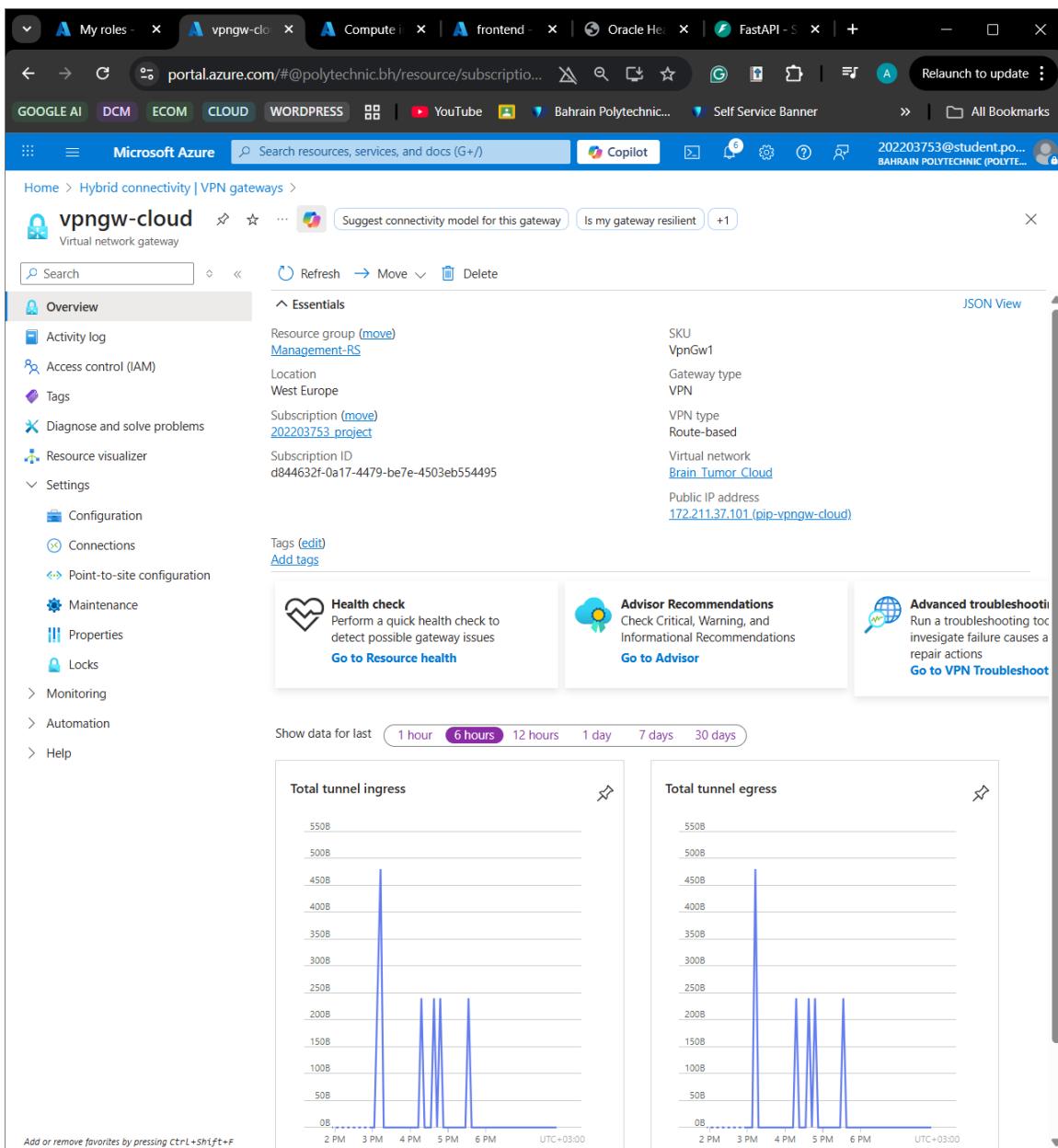


Figure 18: vpngw-cloud dashboard

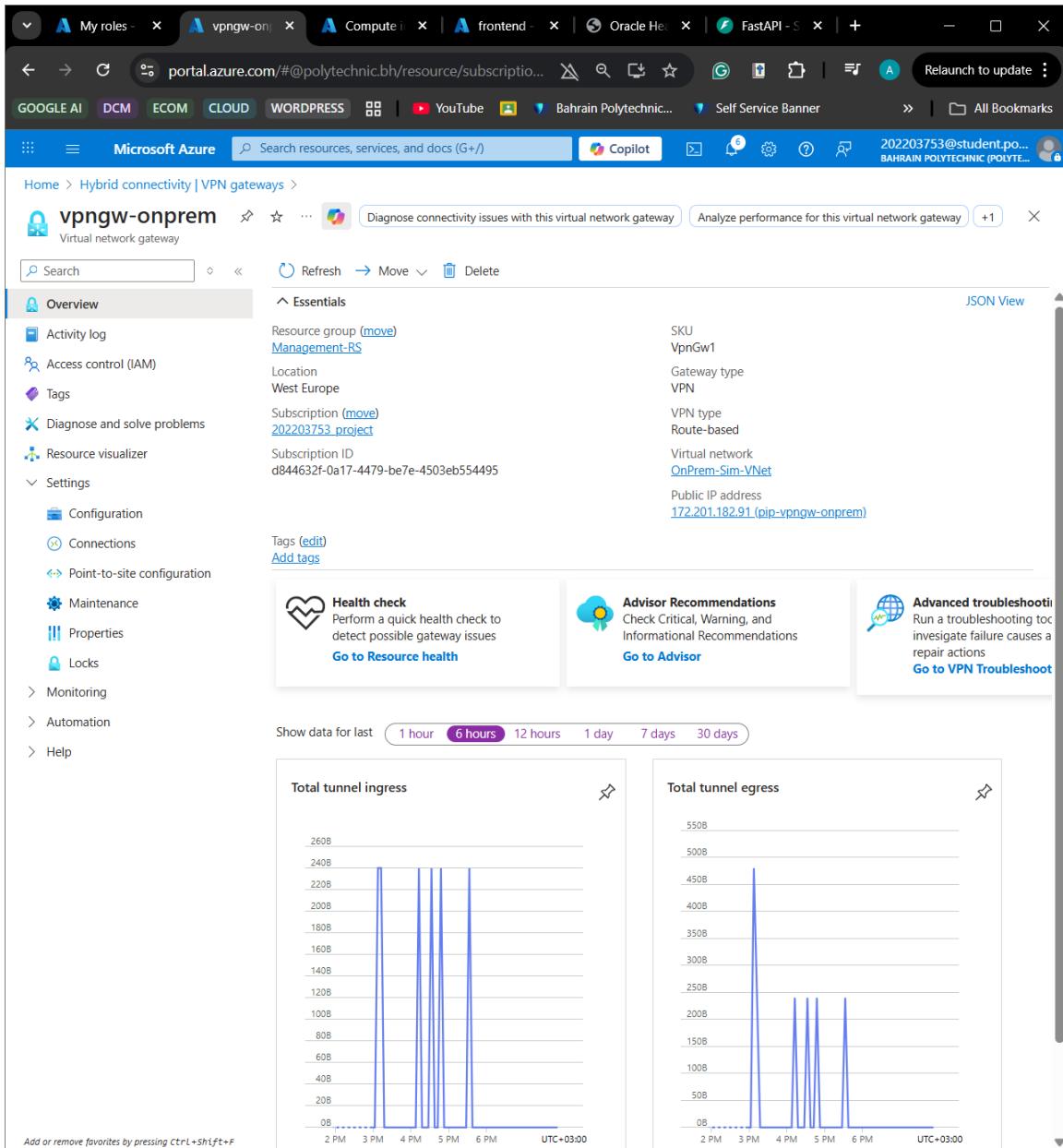
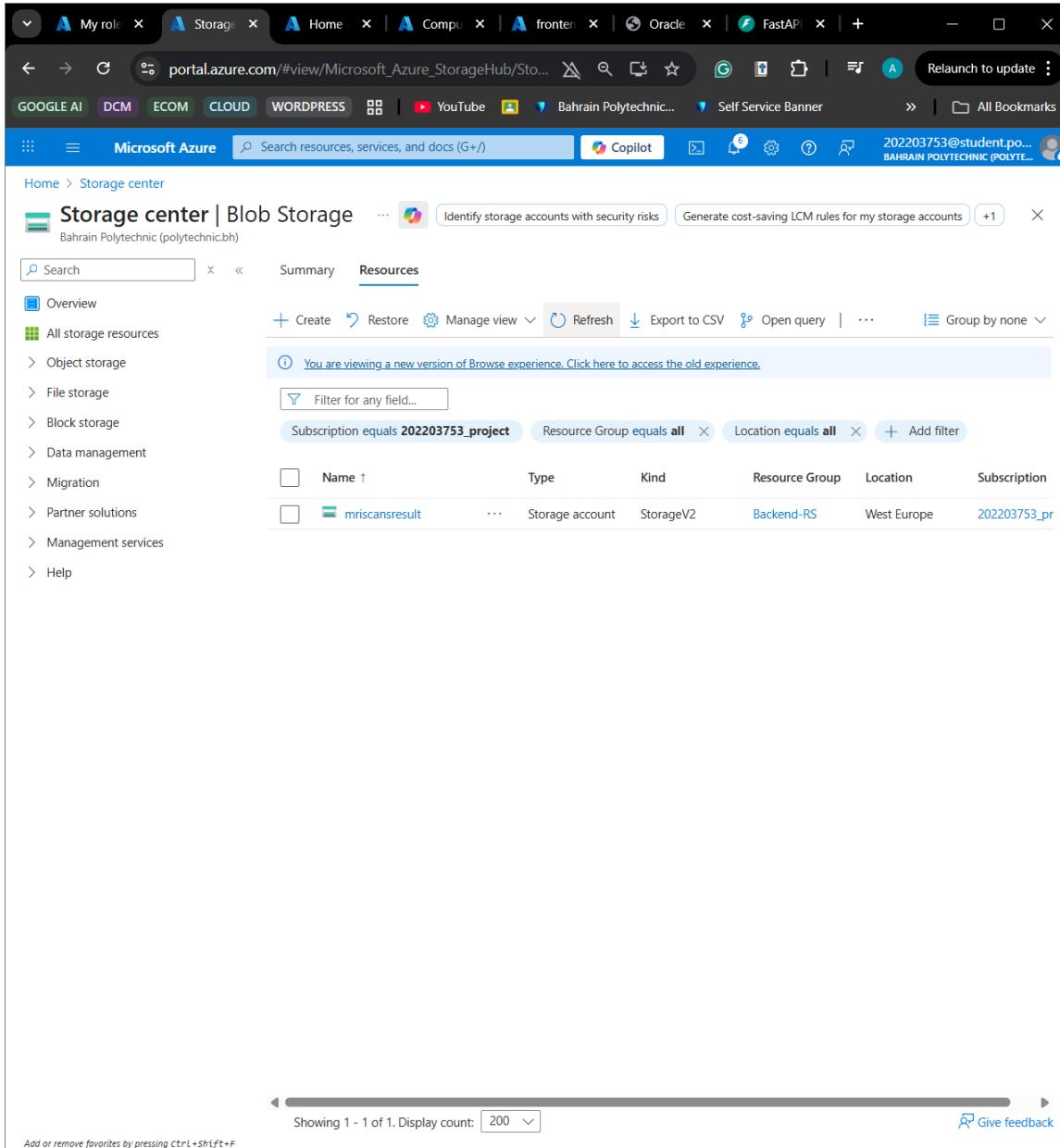


Figure 19: vpngw-onprem dashboard

Storage Implementation

Storage services were designed to facilitate secure processing of medical imaging data, system output, and application artifacts. The selection of the Storage services in Azure was based on their excellent integration with networking, identity, and compliance services in Azure. To ensure all storage resources are in close proximity to the basic infrastructure in Azure, all resources were placed in the same region in Azure and designed to be accessible in a private network only. Public accessibility was blocked, and

role-based access control helped limit permissions to minimize risks to confidentiality, integrity, and availability.



The screenshot shows the Microsoft Azure Storage center interface. The left sidebar lists navigation options: Overview, All storage resources, Object storage, File storage, Block storage, Data management, Migration, Partner solutions, Management services, and Help. The main content area is titled "Storage center | Blob Storage" and shows a table of storage accounts. The table has columns for Name, Type, Kind, Resource Group, Location, and Subscription. One account is listed: "mriscansresult" (Storage account, StorageV2, Backend-RS, West Europe, 202203753_project). There are filters at the top of the table: Subscription equals 202203753_project, Resource Group equals all, and Location equals all. A message at the top says, "You are viewing a new version of Browse experience. Click here to access the old experience." The bottom of the page shows a display count of 200 items.

Figure 20: Storage Account Overview

Blob Storage

The Azure Blob Storage system was set up to handle the files produced by the MRI scanner, the processed images, and the machine learning objects. The storage account was set up to support the usage of private endpoints, and access was restricted to trusted subnets like the ones allocated to the Machine Learning subnet and the Backend subnet. The blob storage

system was selected because it is scalable and cost-effective and supports the uploading of large medical images.

The screenshot shows the Microsoft Azure Blob Storage interface. At the top, there are several browser tabs open, including 'My role', 'mriscansresult', 'Home', 'Compu...', 'fronten...', 'Oracle...', 'FastAPI...', and others. The main navigation bar includes links for 'GOOGLE AI', 'DCM', 'ECOM', 'CLOUD', 'WORDPRESS', 'YouTube', 'Bahrain Polytechnic...', 'Self Service Banner', and 'All Bookmarks'. The user is signed in as '202203753@student.po... BAHRAIN POLYTECHNIC (POLYTE...'.

The current page is 'mriscansresult | Containers'. On the left, a sidebar menu lists various storage-related services: Overview, Activity log, Tags, Diagnose and solve problems, Access Control (IAM), Data migration, Events, Storage browser, Partner solutions, Resource visualizer, Data storage (with 'Containers' selected), File shares, Queues, Tables, Security + networking, Data management, Settings, Monitoring, Monitoring (classic), Automation (with 'Tasks' selected), Export template, and Help. A note at the bottom of the sidebar says 'Add or remove favorites by pressing Ctrl+Shift+F'.

The main content area displays a table of containers:

Name	Last modified	Anonymous access level	Lease state
reports	12/15/2025, 10:48:42 AM	Blob	Available
scan	11/17/2025, 12:22:14 AM	Blob	Available

Figure 21: Blob Storage

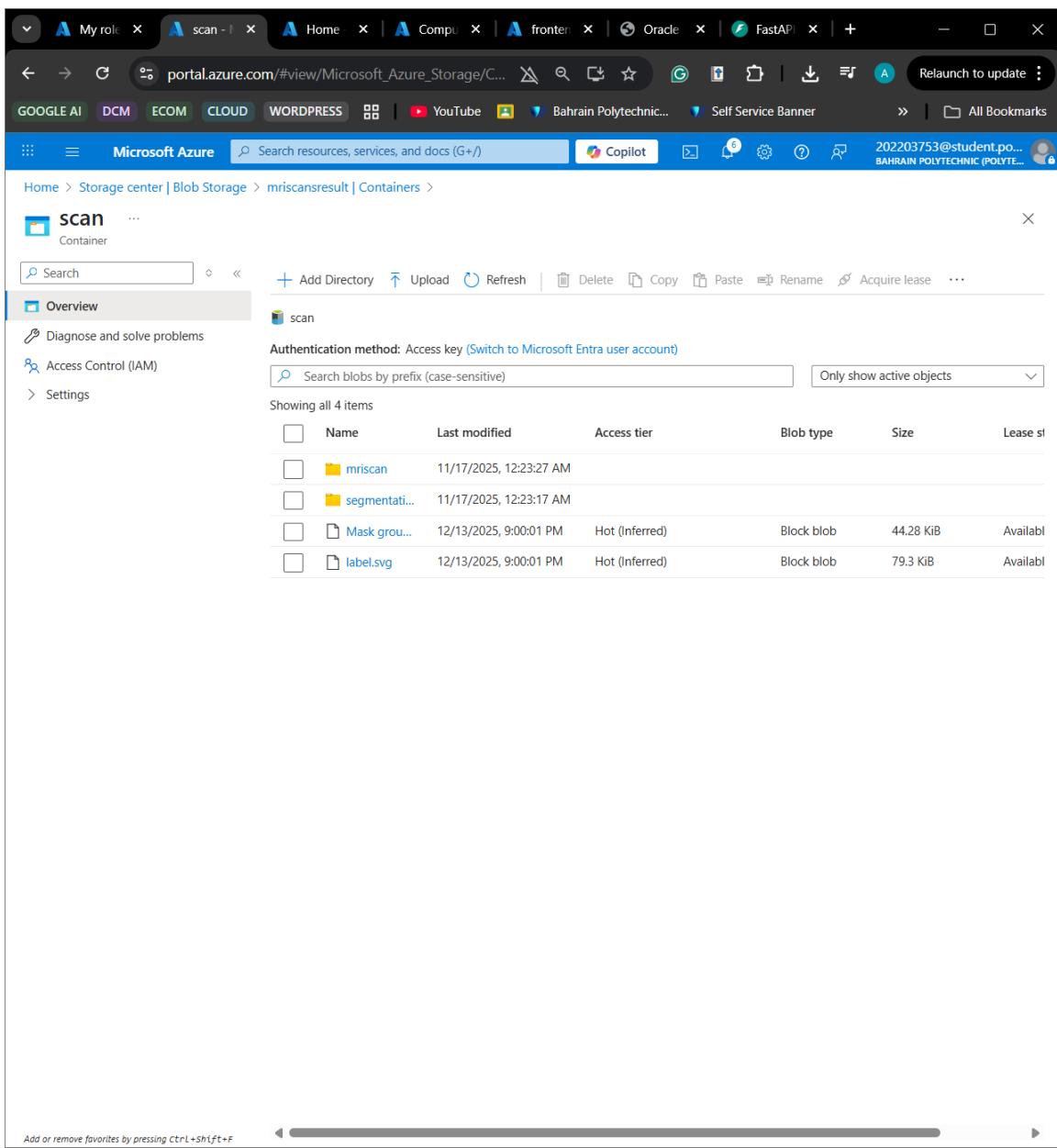


Figure 22: Scans Container Blob Storage

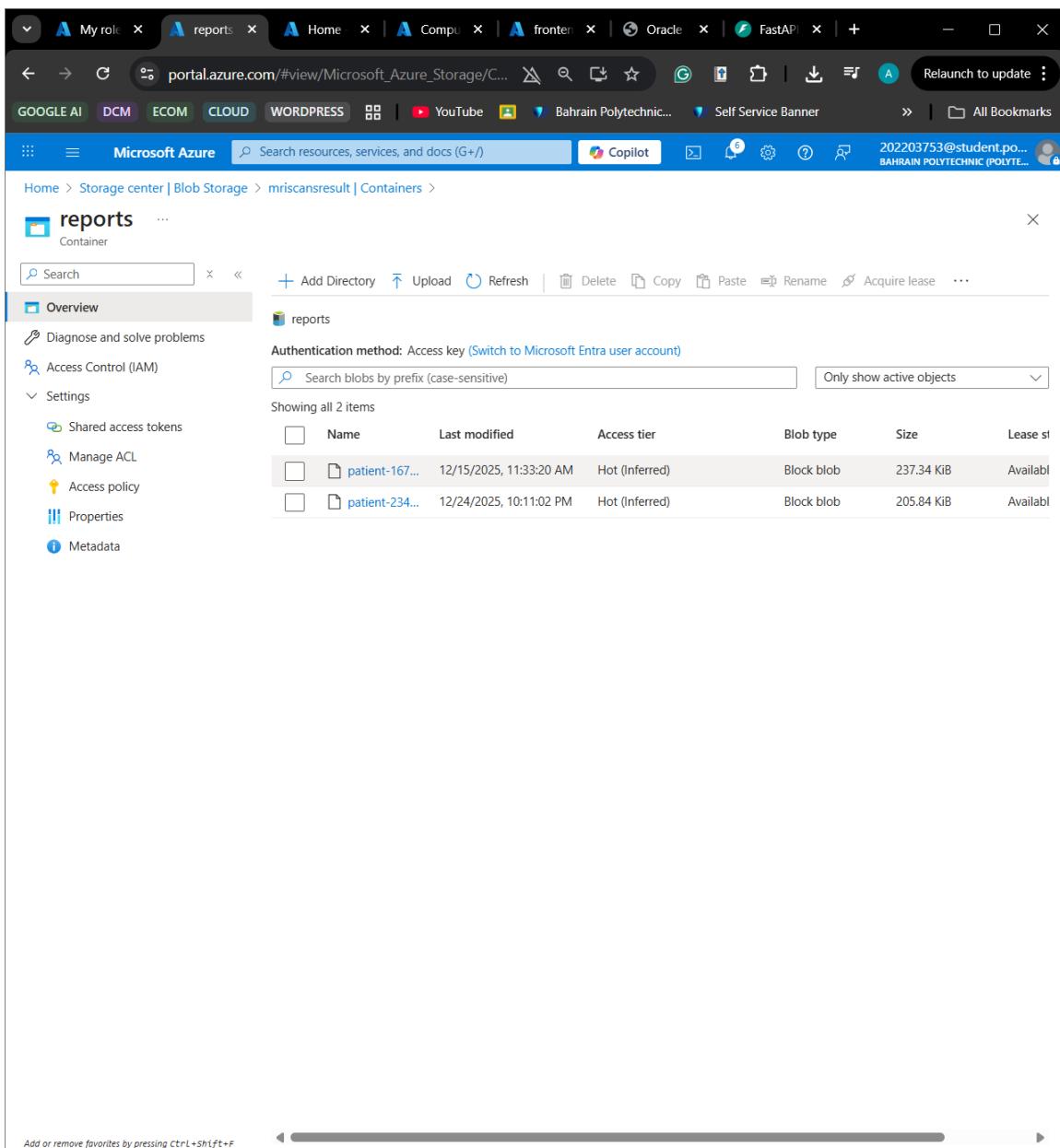


Figure 23: Reports Blob Storage Container

Database Implementation

The database layer, which contains patient metadata, analysis results, and system records, is designed using a managed database service in Azure. The database is hosted on a dedicated subnet without internet access except for the Backend and Machine Learning subnets. The use of a managed service removes administrative overhead in aspects such as backing up, patching, and replication to ensure high availability, thus meeting the system's functional requirements.

The screenshot shows the Microsoft Azure portal interface for managing PostgreSQL databases. The top navigation bar includes links for My role, Azure, Home, Compute, frontends, Oracle, FastAPI, and various service categories like GOOGLE AI, DCM, ECOM, CLOUD, WORDPRESS, and more. The user is signed in as 202203753@student.po... from BAHRAIN POLYTECHNIC (POLYTE...). The main title is "Azure Database for PostgreSQL servers". A message at the top indicates that the "Azure Database for PostgreSQL Single Server" is on the retirement path and the create experience has been retired, suggesting the use of Azure CLI for new instances. Below this, there are filter options: "Subscription equals 202203753_project", "Resource Group equals all", "Location equals all", and a "Add filter" button. The main table lists two database instances:

	Name ↑	Resource type	Status	High availability	Resource Group	Location	Subscription
<input type="checkbox"/>	development-database	Microsoft.DBforP...	Available	Disabled	Backend-RS	West Europe	202203753_proj...
<input type="checkbox"/>	web-db	Microsoft.DBforP...	Stopped	Same zone	Backend-RS	West Europe	202203753_proj...

At the bottom, it says "Showing 1 - 2 of 2. Display count: 200" and a "Give feedback" link.

Figure 24: Database Overview

Model Deployment

The machine learning model was deployed as a containerized inference service using Azure Container Apps. The brain tumor classification model along with its inference logic was packaged into a Docker image and made available over a REST API. The service takes input magnetic resonance imaging (MRI) data provided by the backend application,

performs computations on the inputs using the trained model, and sends back prediction outputs in real-time. The container was running on a private Azure network and allowing communications only from authorized backend components, thus aligning well within the overall system security architecture. Containerization provided a consistent runtime environment for both local and cloud-based testing, eliminating dependency conflicts, and allowing for easy management of model versions and related libraries.

The deployment process involved localized creation of the Docker image, distribution of the image to Azure Container Registry, and deployments on Azure Container Apps, subject to CPU and memory resource limitations. The model parameters, model paths, as well as service ports, were handled using environment variables. This approach allowed for frequent re-deployment in case of changes and also allowed scaling of the machine learning piece without affecting the rest of the application.

Justification on Container-Based Deployment Over ML Workspace

Azure Machine Learning Workspace was initially shortlisted for model deployment, but operationalization under project constraints resulted in unsuccessful deployments. Various technical issues were observed, such as issues with resolving environment images or providing endpoints, that resulted in unsuccessful deployments. Though it was correctly configured, obtaining a stable inference endpoint under the deadline was not achieved.

As a result, the decision was made to implement deployment using containers, which proved more reliable and manageable. The deployment using containers ensured that there was full control over the environment. The process did not rely on managed machine learning endpoints, which was compatible with the infrastructure-orientated nature of the project. Based on that, using containers became identified as the best way forward for a feasible and secure inference service for machine learning within the specific scope and time constraints of the project.

The screenshot shows the Microsoft Azure Container Apps dashboard for the 'mlmodel' application. The left sidebar lists various navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Application, Settings, Networking, Security, Monitoring, Automation, CLI / PS, Export template, and Help. The 'Overview' tab is selected. The main content area displays the 'Essentials' section with the following details:

Setting	Value
Resource group	(move) ML-RS
Status	Running
Location	(move) West Europe
Subscription	(move) 202203753.project
Subscription ID	d844632f-0a17-4479-be7e-4503eb554495
Aspire Dashboard	Not yet active (set up)
Tags	(edit) Container : 555

Below the essentials section, there are three featured sections: 'Discover Azure Container Apps Features'. The first feature is 'Upload artifact' with a 'Upload' button. The second is 'Manage your app with revisions' with a 'View revisions' button. The third is 'Set up continuous deployment' with a 'Set up deployment' button.

Figure 25: ML Container Dashboard

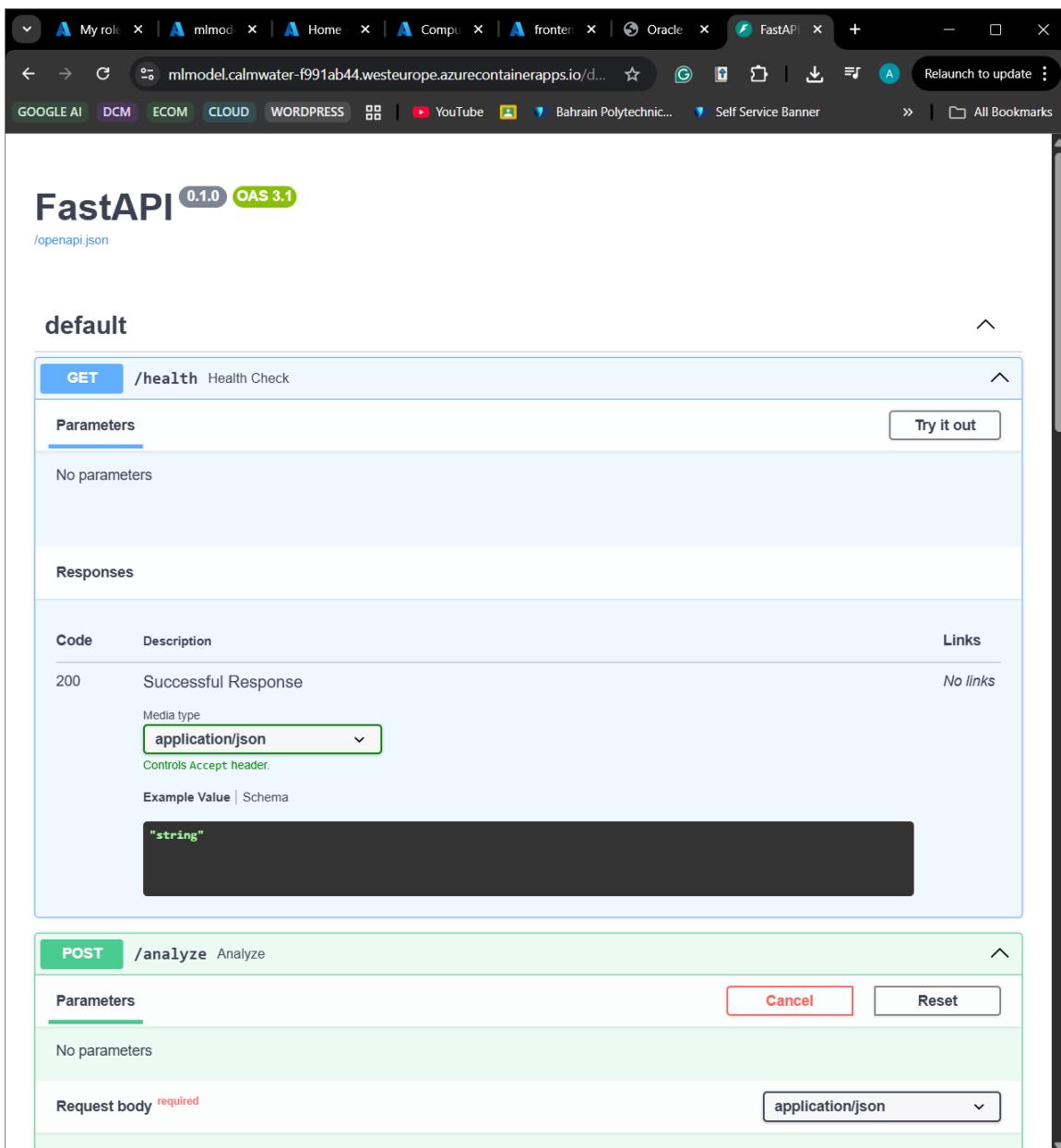


Figure 26: Test URL

Monitoring, Logging & Security Tools

Monitoring, logging, and security controls were implemented to provide continuous visibility into system performance, availability, and security posture. Azure-native monitoring services were selected to allow centralized observation of network traffic, resource utilization, and access activity across all deployed components. Logging was enabled to support auditing, troubleshooting, and compliance verification, particularly for sensitive healthcare data. Security monitoring was integrated with network and compute resources to detect abnormal behavior, failed access attempts, and configuration issues.

This layered monitoring approach supports operational stability and aligns with healthcare data protection requirements.

Azure Monitor

Azure Monitor was configured as the primary monitoring service for the deployed infrastructure. Metrics and logs were collected from virtual networks, subnets, virtual machines, storage accounts, databases, and Azure Machine Learning resources. Diagnostic settings were enabled to capture activity logs, performance metrics, and resource health information. Azure Monitor provides real-time insights into system behavior and supports proactive identification of performance bottlenecks or service disruptions. Centralized dashboards were used to visualize key indicators such as resource availability, network traffic, and error rates, enabling efficient system oversight.

The screenshot shows the Microsoft Azure portal interface with the URL portal.azure.com/#view/Microsoft_Azure_Monitoring/ActivityLog. The left sidebar is collapsed, showing the 'Monitor' section. The main content area is titled 'Monitor | Activity log'. It features a search bar and filter options: 'Management Group : None', 'Subscription : 202203753_project', 'Event severity : All', and 'Timespan : Last 6 hours'. Below these filters is a 'Quick Insights' button. The main table displays 102 items, each with columns for Operation name, Status, Time, Time stamp, Subscription, and Event initiated by. The table lists various Azure API operations such as 'Write Role assignment schedule', 'Create role assignment', 'Validate', 'Delete Storage Account', and 'List Storage Account Keys'. Most operations are successful, with some being accepted or failed. The 'Event initiated by' column shows email addresses like '202203753@student.polyt...' and 'MS-PIM'. At the bottom of the table, there is a note: 'Add or remove favorites by pressing Ctrl+Shift+F'.

Operation name	Status	Time	Time stamp	Subscription	Event initiated by
> <i>i</i> Write Role assignment schedule	Succeeded	8 minutes ago	Sat Dec 27 ...	202203753_project	202203753@student.polyt...
> <i>i</i> Create role assignment	Succeeded	8 minutes ago	Sat Dec 27 ...	202203753_project	MS-PIM
> <i>i</i> Validate	Succeeded	8 minutes ago	Sat Dec 27 ...	202203753_project	202203753@student.polyt...
> <i>i</i> Delete Storage Account	Succeeded	13 minutes ago	Sat Dec 27 ...	202203753_project	202203753@student.polyt...
> <i>i</i> Remove member from role (PIM a	Succeeded	15 minutes ago	Sat Dec 27 ...	202203753_project	202203753@student.polyt...
> <i>i</i> Delete role assignment	Succeeded	15 minutes ago	Sat Dec 27 ...	202203753_project	MS-PIM
> <i>i</i> List Storage Account Keys	Succeeded	24 minutes ago	Sat Dec 27 ...	202203753_project	202203753@student.polyt...
> <i>i</i> List Storage Account Keys	Succeeded	24 minutes ago	Sat Dec 27 ...	202203753_project	202203753@student.polyt...
> <i>i</i> Create or Update Load Balancer	Succeeded	32 minutes ago	Sat Dec 27 ...	202203753_project	Microsoft Azure Legion
> <i>i</i> Create or Update Load Balancer	Succeeded	42 minutes ago	Sat Dec 27 ...	202203753_project	Microsoft Azure Legion
> <i>i</i> Auth Token for Container App Dev	Succeeded	42 minutes ago	Sat Dec 27 ...	202203753_project	202203753@student.polyt...
> <i>i</i> Auth Token for Container App Dev	Succeeded	46 minutes ago	Sat Dec 27 ...	202203753_project	202203753@student.polyt...
> <i>i</i> Create or Update Container App	Accepted	47 minutes ago	Sat Dec 27 ...	202203753_project	202203753@student.polyt...
> <i>i</i> Auth Token for Container App Dev	Succeeded	48 minutes ago	Sat Dec 27 ...	202203753_project	202203753@student.polyt...
> <i>i</i> Create or Update Container App	Succeeded	52 minutes ago	Sat Dec 27 ...	202203753_project	202203753@student.polyt...
> <i>i</i> List Container Registry Login Cred	Succeeded	52 minutes ago	Sat Dec 27 ...	202203753_project	202203753@student.polyt...
> <i>i</i> Delete Container App	Succeeded	55 minutes ago	Sat Dec 27 ...	202203753_project	202203753@student.polyt...
> <i>i</i> List Container Registry Login Cred	Succeeded	60 minutes ago	Sat Dec 27 ...	202203753_project	202203753@student.polyt...
> <i>i</i> Create or Update Container App	Accepted	an hour ago	Sat Dec 27 ...	202203753_project	202203753@student.polyt...
> <i>i</i> Create or Update Container App	Accepted	an hour ago	Sat Dec 27 ...	202203753_project	202203753@student.polyt...

Figure 27: Monitor | Activity Log

5. Testing

Test Plan

The test plan has been designed to ascertain that the implemented Azure infrastructure meets the functional, security, and operational needs described in the project plan. The test exercise had the objective to, among other things, ensure the correct implementation of networking elements, restricted connectivity between the subnets, secured data storage, and successful communication between the web app, machine learning module, and the database layer. Every test scenario has been conducted after the infrastructure has been deployed.

The test scenarios defined within the project plan were systematically implemented. These tests included checking for connections between approved subnets, checking for blocked transmissions on restricted sites, checking private access to storage and DB services, and checking monitoring/logging services to ensure system activity logs were being recorded. There are additional tests performed to ensure service functionality as well as basic fail-over processes. These tests were defined as pass or fail, and any tests that failed were remedied by changing system configurations.

Participants

The test activities were undertaken by the participants who were identified by the project plan. The project implementer was largely responsible for the testing of the cases, which included all the infrastructure tests carried out on the Azure platform. The project supervisor acted as the checker of the test cases to ensure that they are carried out according to the goal of the project.

Participant	Age	Gender	Background	Skills and Role in Testing
Ali AlRashedi	20	Male	An Information Systems student with the basics of cloud computing and experience in the design and implementation of Azure-based cloud infrastructure, virtual networks, subnets, and security features.	test cases related to the networking and security aspects have been performed, ranging from subnet isolation, NSG rule validation, private access, to the validation of the restricted communications between the services.
Ali Almuzayen	22	Male	An Information Systems student with expertise in cloud computing and awareness of machine learning paradigms and processes involving model deployment and services.	Machine learning test cases were also performed to confirm the accessibility of the ML, the secure connectivity to the storage and database, and the successful execution of models.
Hussain Mohammed Ali	22	Male	An Information Systems student with knowledge in database management and programming. Manage databases, controlling data access and app logic integration. Programming expertise aided in backend service implementation, facilitating communication between the cloud infrastructure and database component.	Test cases have been conducted on the database backend, including connectivity, access validation, data flow, and secure communication with the application services.

Table 4: Participants in Test Cases

Functional Requirements Test Cases and Results

This section details how the functional requirements of the system have been verified through structured test cases, as projected in the project plan. All test cases were also used to ensure that all functional requirements related to the cloud infrastructure work as expected under normal working conditions. The test cases did not include application logic but emphasized safe connectivity and service interaction.

All the test cases were run as soon as the infrastructure had been fully implemented. Test results are tabulated below, outlining the aim of the tests, the phases of execution, and the expected and actual results with pass and fail indicators. In executing tests, step-by-step images of progressive implementations were taken as graphical representation of proper functioning of the system.

Test Case ID	Test Scenario	Test Case	Test Steps	Test Data	Expected Result	Actual Result	Status (Pass/Fail)
1	Verify MRI upload	Upload MRI image to cloud	1. Click upload 2. Choose the MRI image. 3. Submit	MRI image (.jpg/.png)	MRI uploaded to blob storage	Image was uploaded to Blob storage	PASS
2	Check tumor analysis	Process uploaded MRI	1. Click analyze 2. Wait for process	Stored MRI image	Tumor detected successfully	When model was containerized and image was taken and uploaded	PASS
3	Check result display	View analyzed MRI result	1. Open results page 2. View image	Processed image	Tumor area shown clearly	ML model only gave a yes and no if there was Tumor or not	PARTIALLY
4	Check reports	Download	1. Click download	Report file	Report	Though it was not tested, but results	Not TESTED

	download	result report	report 2. Save file		downloaded	were found in Blob Storage	
5	Check cloud backup	Backup MRI data	1. Start backup 2. Wait for finish	MRI data	Backup completed	Not tested due to budget reasons	Not Tested
6	Check data security	Ensure uploaded data is encrypted	1. Upload MRI 2. Observe network	Encrypted data	Data sent securely	A Site-to-Site VPN was used to securely upload data.	Pass
7	Check failover	Restore system after crash	1. Simulate crash 2. Run recovery	System data	System restored	Due to budget reasons, costs failover was not tested	Not Tested/failed
8	Check user access	Test admin and user roles	1. Log in as admin 2. Log in as user	User credentials	Admin has full access, user limited	Website fully functional though user test cases were not tested	PARTIALLY
9	Check system monitoring	Verify alerts and usage tracking	1. Open Azure Monitor 2. Check logs	System data	Alerts appear correctly	Alerts did not appear but, logs were showing what is happening to the resources	PASS

Table 5: Functional Requirements Test Case

Network and Connectivity Test Cases Results

This paragraph verifies the functional requirements for virtual networking configuration as well as connectivity between subnets. The test scenarios covered in this paragraph test whether authorized communication routes between the subnets are allowed while any unlawful traffic is restricted. All these tests validate whether the network segmentation functionalities of the Azure Virtual Network are correctly implemented.

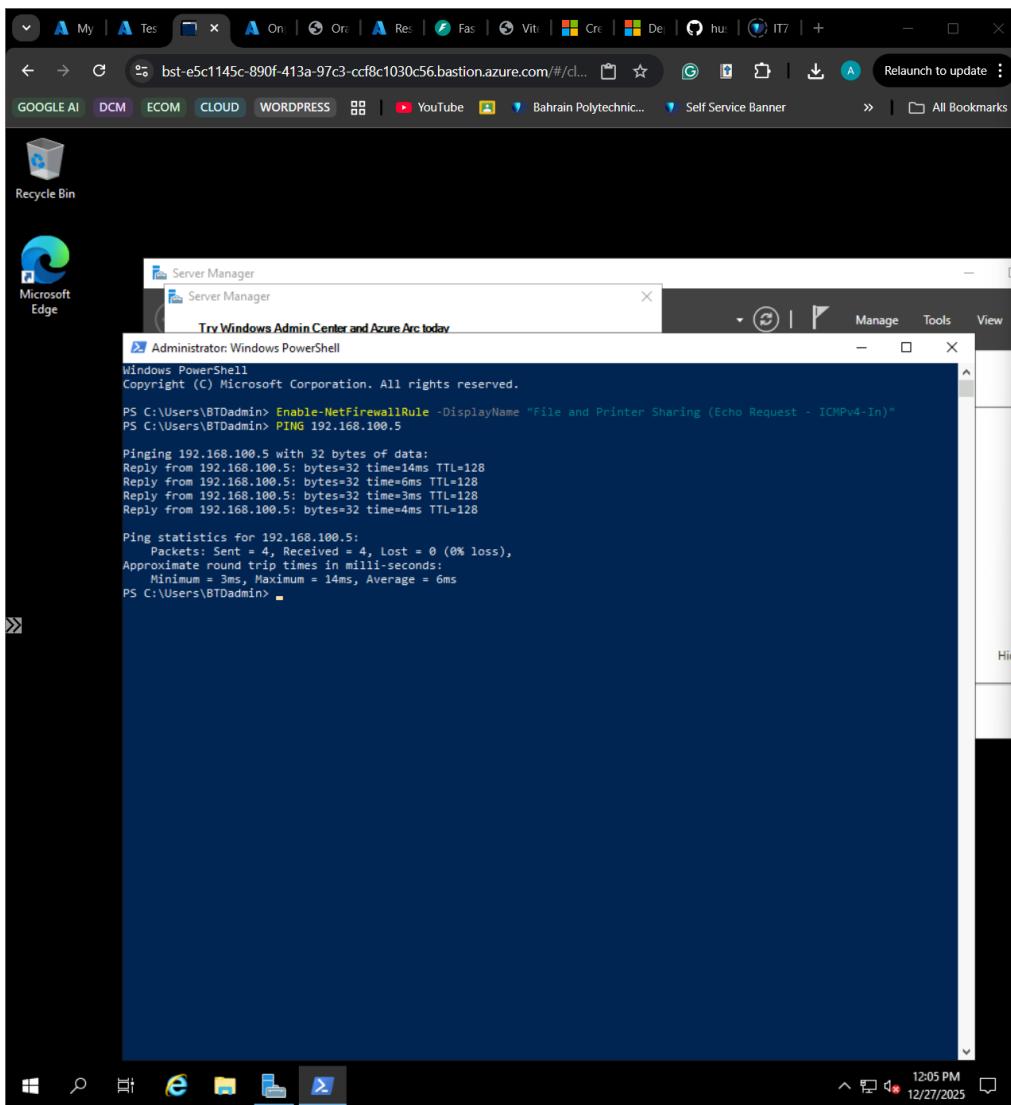
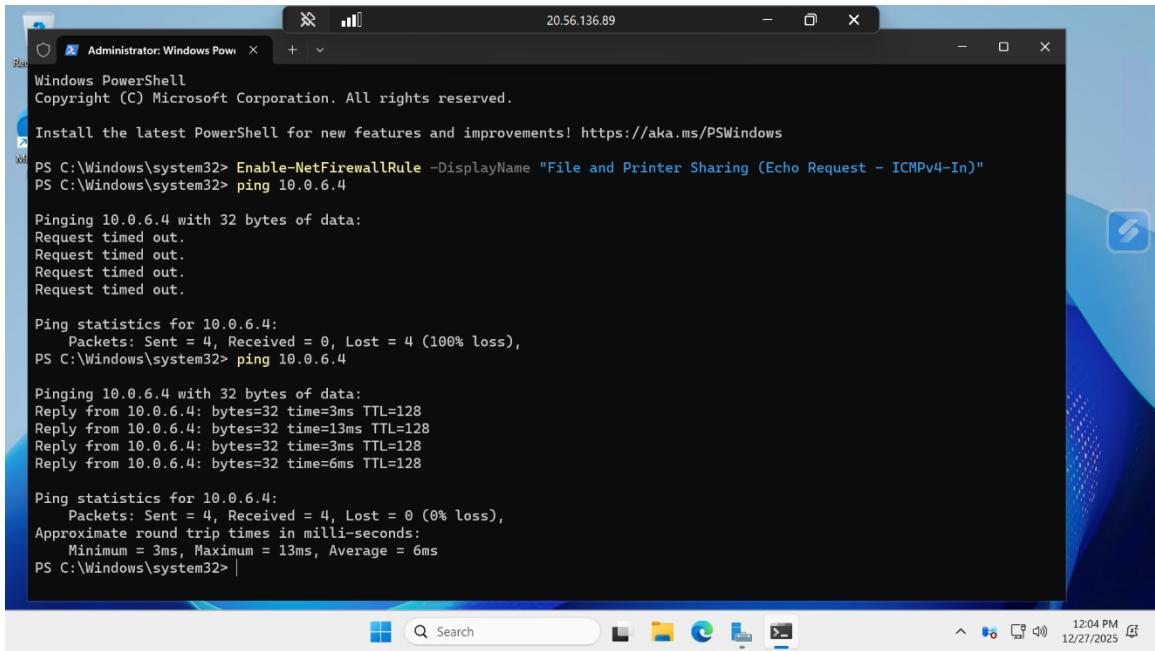


Figure 28: Bastion Ping to simulated on Premises



The screenshot shows a Windows PowerShell window titled "Administrator: Windows Pow" with the IP address "20.56.136.89" in the title bar. The command "Enable-NetFirewallRule -DisplayName "File and Printer Sharing (Echo Request - ICMPv4-In)" was run, followed by a ping command to the IP address 10.0.6.4. The output shows multiple failed pings due to a firewall rule, followed by a successful ping with statistics: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Minimum = 3ms, Maximum = 13ms, Average = 6ms.

```
Administrator: Windows Pow 20.56.136.89
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> Enable-NetFirewallRule -DisplayName "File and Printer Sharing (Echo Request - ICMPv4-In)"

PS C:\Windows\system32> ping 10.0.6.4

Pinging 10.0.6.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.6.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Windows\system32> ping 10.0.6.4

Pinging 10.0.6.4 with 32 bytes of data:
Reply from 10.0.6.4: bytes=32 time=3ms TTL=128
Reply from 10.0.6.4: bytes=32 time=13ms TTL=128
Reply from 10.0.6.4: bytes=32 time=3ms TTL=128
Reply from 10.0.6.4: bytes=32 time=6ms TTL=128

Ping statistics for 10.0.6.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 13ms, Average = 6ms
PS C:\Windows\system32>
```

Figure 29: Success Ping from On Premises to Cloud Bastion VM

Security and Access Control Test Cases Results

The security-related functionality tests form the main concern of this subsection. The test cases are made to make sure that the Network Security Groups provide adequate restrictions for inbound and outbound networks as well as the prevention of public access and the provision of private access to storage and database resources. The main objective for tests is to ensure the fulfillment of the security requirements mentioned in the project plan.

Web_App_NSG Network security group

Overview

Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Settings (Inbound security rules, Outbound security rules), Network interfaces, Subnets, Properties, Locks, Monitoring, Automation, Help.

Essentials

Resource group ([move](#)) Management-RS, Location West Europe, Subscription ([move](#)) 202203753 project, Subscription ID d844632f-0a17-4479-be7e-4503eb554495, Tags ([edit](#)) NSG-Tag : 14, Custom security rules 1 inbound, 0 outbound, Associated with 1 subnets, 0 network interfaces.

Inbound Security Rules

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination
100	Allow_AppGateway_C...	65200-65535	Any	Any	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetw...
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

Outbound Security Rules

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetw...
65001	AllowInternetOutBound	Any	Any	Any	Internet
65500	DenyAllOutBound	Any	Any	Any	Any

Figure 30: Web NSG Inbound and Outbound Security Rules

Storage and Data Test Cases Results

The functional requirements with respect to storage and access of data are examined in this section. The test cases are designed to check that access from untrusted services is denied and that access to Azure Blob Storage is possible only from authorized services and subnets.

The screenshot shows the Microsoft Azure Activity Log for the storage account 'mriscansresult'. The left sidebar lists various categories like Overview, Activity log, Tags, Diagnose and solve problems, Access Control (IAM), Data migration, Events, Storage browser, Partner solutions, Resource visualizer, Data storage (Containers, File shares, Queues, Tables), Security + networking, Data management, Settings, Monitoring, Monitoring (classic), Automation (Tasks, Export template), and Help. The 'Activity log' tab is selected. The main pane displays a table of activity logs with columns: Action, Status, Time, Date, and ID. Most actions are 'Succeeded', while one is 'Failed'. The log includes entries for listing storage account keys, putting blob containers, deleting blob containers, and listing storage account keys again.

Action	Status	Time	Date	ID
> List Storage Account Keys	Succeeded	5 days ago	Mon Dec 22 2025 22:0...	202203753_project
> List Storage Account Keys	Succeeded	2 weeks ago	Mon Dec 15 2025 11:4...	202203753_project
> List Storage Account Keys	Succeeded	2 weeks ago	Mon Dec 15 2025 11:4...	202203753_project
> Put blob container	Succeeded	2 weeks ago	Mon Dec 15 2025 10:4...	202203753_project
> Put blob container	Succeeded	2 weeks ago	Mon Dec 15 2025 10:4...	202203753_project
> Put blob container	Failed	2 weeks ago	Mon Dec 15 2025 10:4...	202203753_project
> Delete blob container	Succeeded	2 weeks ago	Mon Dec 15 2025 10:4...	202203753_project
> List Storage Account Keys	Succeeded	2 weeks ago	Mon Dec 15 2025 10:4...	202203753_project
> List Storage Account Keys	Succeeded	2 weeks ago	Mon Dec 15 2025 10:4...	202203753_project
> List Storage Account Keys	Succeeded	2 weeks ago	Sat Dec 13 2025 20:59:...	202203753_project
> List Storage Account Keys	Succeeded	2 weeks ago	Sat Dec 13 2025 20:59:...	202203753_project
> List Storage Account Keys	Succeeded	2 weeks ago	Thu Dec 11 2025 17:33:...	202203753_project
> List Storage Account Keys	Succeeded	2 weeks ago	Thu Dec 11 2025 17:33:...	202203753_project
> List Storage Account Keys	Succeeded	2 weeks ago	Thu Dec 11 2025 17:21:...	202203753_project
> List Storage Account Keys	Succeeded	2 weeks ago	Thu Dec 11 2025 16:11:...	202203753_project
> List Storage Account Keys	Succeeded	2 weeks ago	Thu Dec 11 2025 16:11:...	202203753_project
> List Storage Account Keys	Succeeded	2 weeks ago	Thu Dec 11 2025 16:04:...	202203753_project
> List Storage Account Keys	Succeeded	2 weeks ago	Thu Dec 11 2025 16:04:...	202203753_project
> List Storage Account Keys	Succeeded	2 weeks ago	Thu Dec 11 2025 13:26:...	202203753_project
> List Storage Account Keys	Succeeded	2 weeks ago	Thu Dec 11 2025 13:26:...	202203753_project
> List Storage Account Keys	Succeeded	2 weeks ago	Thu Dec 11 2025 13:25:...	202203753_project
> List Storage Account Keys	Succeeded	2 weeks ago	Thu Dec 11 2025 13:25:...	202203753_project
> List Storage Account Keys	Succeeded	2 weeks ago	Thu Dec 11 2025 13:25:...	202203753_project
> List Storage Account Keys	Succeeded	2 weeks ago	Thu Dec 11 2025 13:25:...	202203753_project
> List Storage Account Keys	Succeeded	2 weeks ago	Thu Dec 11 2025 13:25:...	202203753_project
> List Storage Account Keys	Succeeded	2 weeks ago	Thu Dec 11 2025 13:25:...	202203753_project
> List Storage Account Keys	Succeeded	3 weeks ago	Thu Dec 04 2025 14:55:...	202203753_project
> List Storage Account Keys	Succeeded	3 weeks ago	Thu Dec 04 2025 14:55:...	202203753_project
> List Storage Account Keys	Succeeded	3 weeks ago	Thu Dec 04 2025 14:55:...	202203753_project

Figure 31: Logs Of Recent Activities on Storage Account

Database Connectivity Test Cases Results

This subsection evaluates the functional need to access the database. Test cases will ensure that operations on the data are functioning correctly by testing that only trusted backend and machine learning services can access the database, but public database connectivity is disabled except in the case of an experimental database.

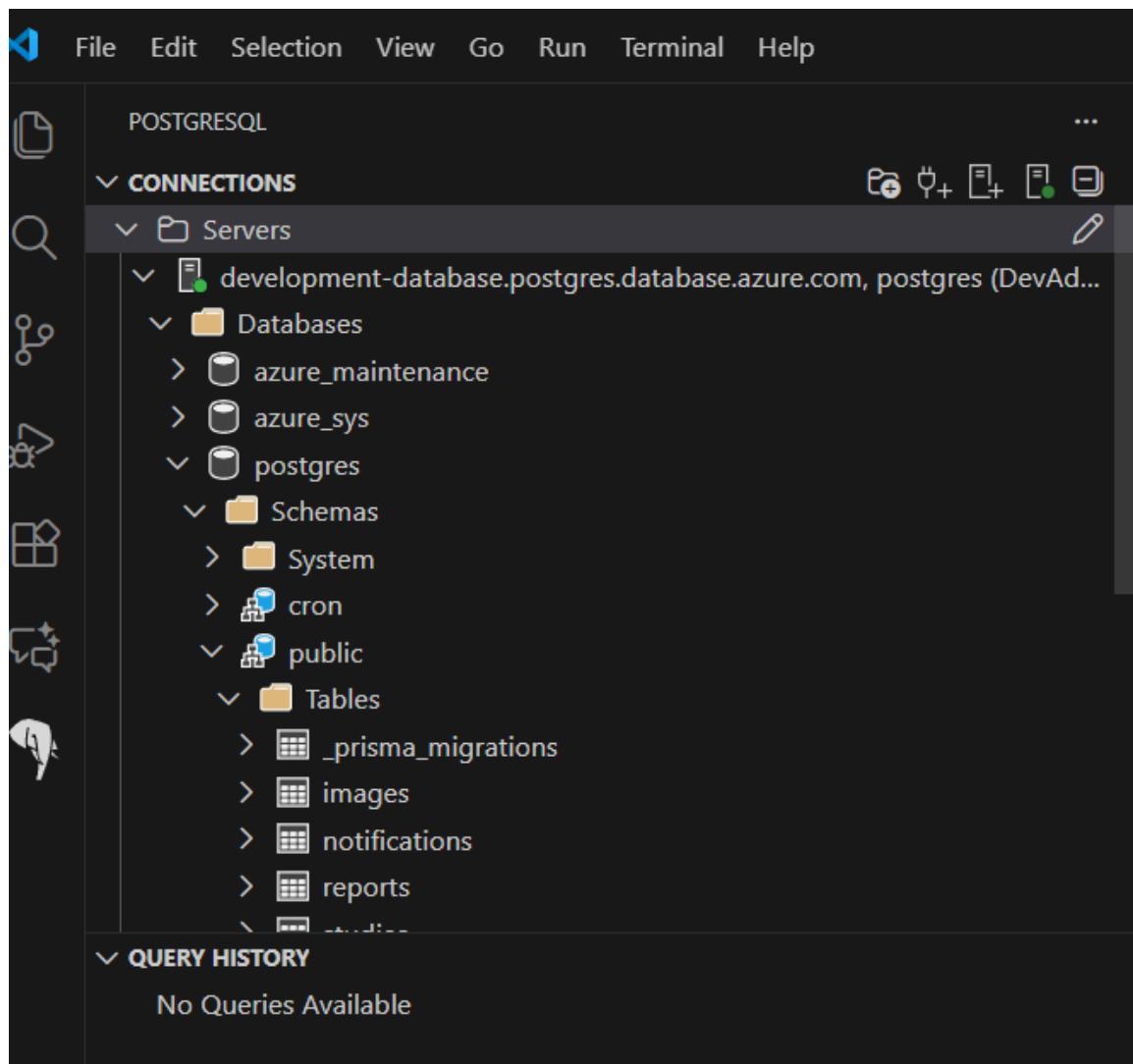


Figure 32: Active Database Connection (Development DB)

Acceptance Test Process and Results

Acceptance testing was performed in order to test that the developed system meets the specified user requirements and project goals. Test scenarios were taken from test cases in project plan operational scenarios developed during the engineering and design phases. The goal of such acceptance testing was focused on testing of the developed system from a stakeholder point of view, mostly with respect to functionality, security, and availability.

Every acceptance test was performed in the Azure environment. The result of the test would be captured as Pass, Partial Pass, and Fail upon fulfillment of certain acceptance criteria.

If required, screen shots would be captured to ensure evidence of the test execution and system behavior.

It is evident from the overall results that the system satisfied most of its acceptance criteria. Small performance constraints have been noticed during the simulation tests of workload, mainly owing to limited computational resources. These constraints do not impact the basic functionality of the system and shall be overcome in future scaling

Test ID	Participant	Process	Status	Justification of the Result
1	Ali AlRashedi	Test Site-to-Site VPN connectivity between on-premises network and Azure Vnet.	Pass	VPN tunnel established successfully with encrypted traffic and stable connectivity.
2	Ali AlRashedi	Validate Azure Virtual Network and subnet deployment.	Pass	VNets and subnets were deployed according to the approved IP addressing scheme.
3	Ali AlRashedi	Verify traffic isolation using Network Security Groups	Pass	Only permitted ports and protocols were allowed, blocking unauthorized traffic.
4	Hussain Mohmmmed Ali	Test Azure Blob Storage access for medical image storage	Pass	Files were uploaded and retrieved successfully.
5	Hussain Mohmmmed Ali	Validate database connectivity	Pass	Database was reachable
6	Ali AlRashedi	Test system availability under normal workload Screenshot	Pass	System services remained stable and responsive during normal operation.
7	Ali Almuzayen	Tested ML model by uploading an image to test accuracy	Partial Pass	Model works fine on container although design requirement mentioned was on Azure ML workspace

Table 6: Acceptance Test Process Results

Usability Testing Results and Statistics

Responsiveness, reliability, and ease of use were evaluated by usability testing the system's response using Azure-monitoring tools and respective metrics. The testing was performed by uploading data to the Azure Blob Storage service, downloading the stored results, and tracking back-end and database operations using Azure Monitor dashboards. All tasks were

done via Azure Portal interfaces, signifying that the system can be readily used and learned by an administrator.

The performance metrics ensure that the solution is stable during the period of testing. The metrics for the blob storage solution indicate low ingress and egress traffic, stable request processing, and an average latency of about 78ms, thus enabling fast data access. The metrics for the PostgreSQL database indicate a stable number of active connections, averaging between 6-7 connections, with no unusual spikes or downtime. Error rates remain very low and limited to the initial setting stages. Overall, the outcome of the metrics demonstrates the stability and simplicity of the solution as well as the usability requirements set for the respective project.

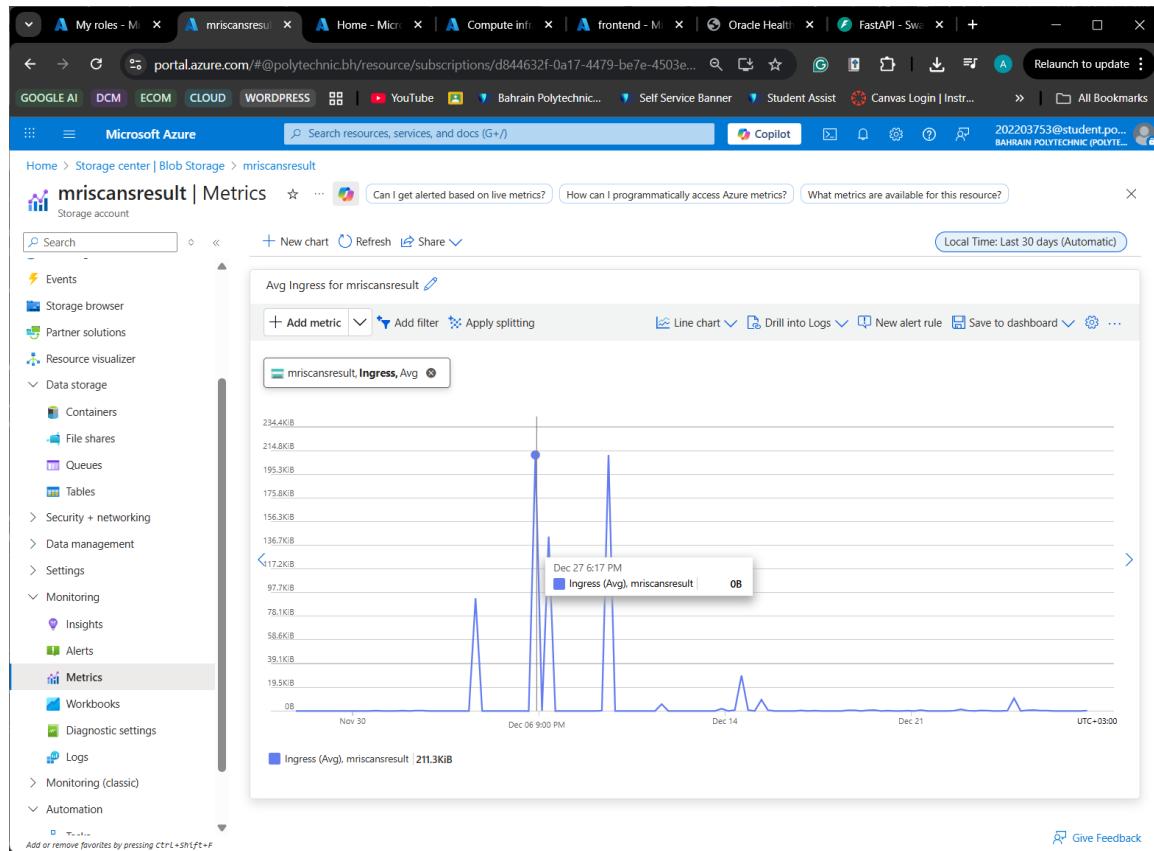


Figure 33: Blob Storage Performance Metrics on Ingress

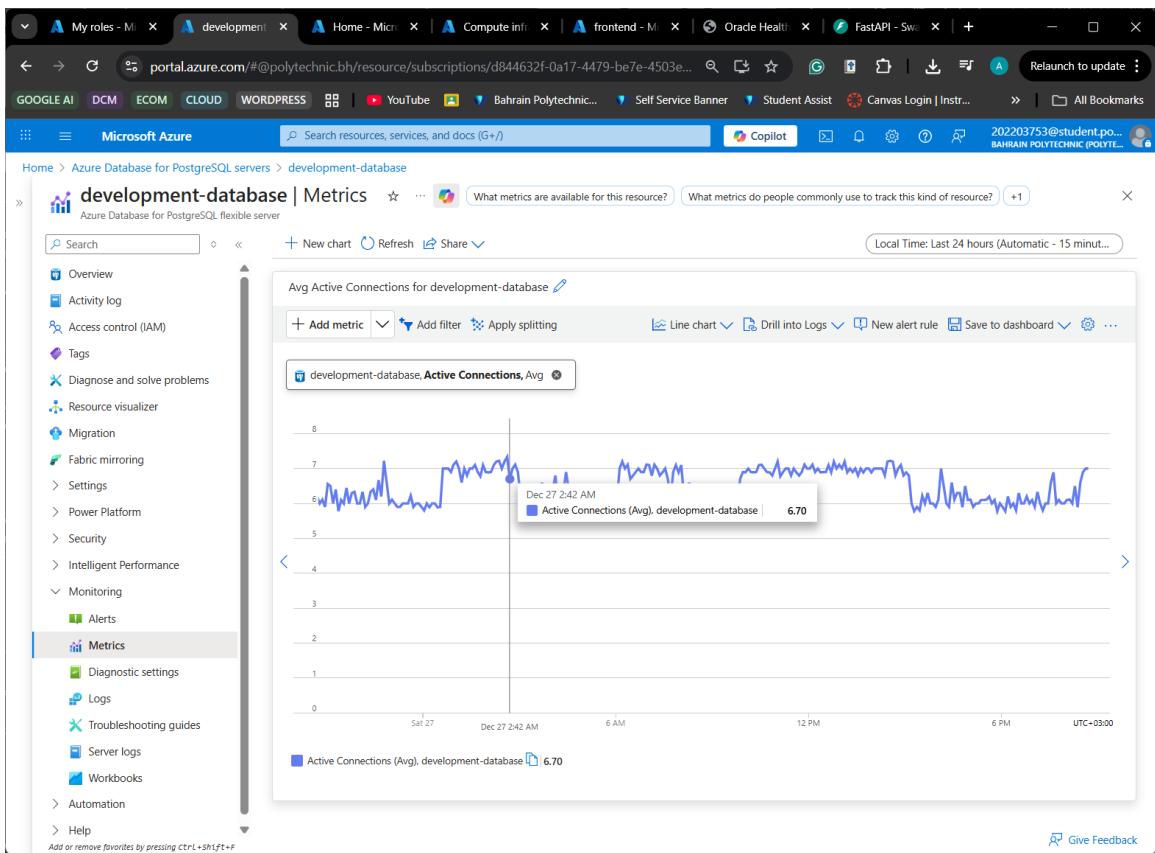


Figure 34: PostgreSQL Database Active Connections

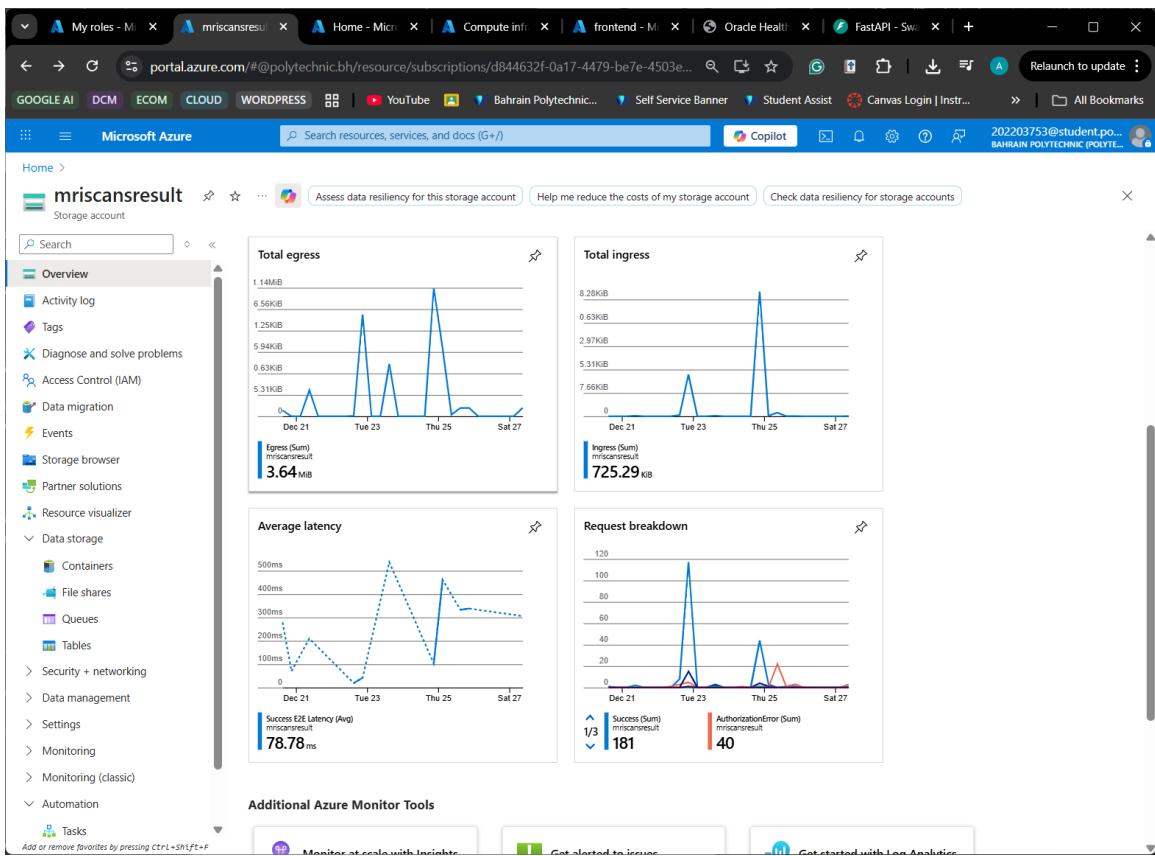


Figure 35: Blob Storage Performance and Statistics on Ingress, egress, latency, and Request metrics

6. Discussion, LESPI, and Conclusion

This section outlines the findings of the project in terms of cloud infrastructure in the healthcare system. The primary focus of this section will be on the cloud infrastructure setup in this project, highlighting the support of secure data management, restricted access, and stable service operations in medical applications through the Azure architecture setup. This section emphasizes the infrastructure setup rather than application logic. Moreover, the limitations in the existing setup also trigger the future improvements discussed in the next section.

System Functionality

The provisioned cloud infrastructure behaved as intended and addressed key functional needs identified in the project plan. The design of the private Virtual Network in Azure was appropriately used to provide network segmentation of healthcare workloads in separate subnets. Network Security Groups, in collaboration with private connectivity features, were used to provide adequate access control to avoid exposure of sensitive healthcare data to the general Internet.

The storage and database services were functioning in a closed network environment that facilitated secure data communication between the approved components of the system. The Azure monitoring and logging service also ensured adequate visibility of the infrastructure and access to it. The combined effect of the infrastructure proved that it is able to provide healthcare-related cloud services.

Accomplished Objectives

The main goal of the project has been achieved by developing an appropriate cloud architecture that is secure and structured enough to be utilized within the healthcare environment. A structured test has ensured that the infrastructure goal of the architecture is met as far as the segmentation of the network, private data storage, and monitoring of the services are concerned.

Besides, it fulfilled another requirement by providing a starting platform to which additions could be made by future releases. While the current implementation prioritizes correctness,

security, and access controls, a foundation has been laid for adding more advanced features regarding scalability, redundancy, and automation, as shall be clarified below.

Technical and Business Objectives

The goal of the project was to offer a safe and efficient cloud infrastructure supporting healthcare systems, while maintaining their operational efficiency. From a technical standpoint, it was a challenge to develop an efficient and safe cloud infrastructure that is capable of supporting medical applications. On a business standpoint, it is evident that cloud infrastructure can also be deployed effectively and economically in the healthcare sector.

From a Technical perspective, some of the objectives achieved:

- Building a segmented virtual network in Azure to isolate healthcare workloads
- Least privilege access via Network Security Groups and Private Endpoints
- Data Storage and Database Services Security inside the Private Network Borders
- Integration with native Azure services to enable management without compromising security controls

One of the objectives that was not met was the use of Azure ML Workspace to host ML models, for that, Azure Container Apps were considered as an alternative solution to it.

Despite the accomplishment of these goals, several advanced features for the infrastructure had been intentionally excluded for reasons of project feasibility and resource availability.

These exclusions include the following:

- redundancy over multiple regions
- automatic scalability
- advanced security analytics capabilities.

Excluding these does not make the solution imperfect but ensures technical development paths for improvement outlined in the Future Plan section.

In terms of business and operations, the target was:

- Lower operational overheads through managed usage of cloud infrastructure
- Scalable architecture that facilitates the gradual growth of the overall system
- Offer a cloud-based system that requires minimal infrastructure costs
- Enhance maintainability and efficient operation. The existing design focuses more on its operational feasibility rather than its ability to be fully productive.

With the evolving nature of the requirement for healthcare services, high availability, scalability, and accessibility are becoming increasingly crucial, which are emphasized through the Future Plan and Work mentioned.

Project Issues

The deployment of the cloud infrastructure faced a series of technical and configuration issues. The majority of the issues were evident as a result of the challenges encompassing the integration of multiple services from the Azure platform in a private healthcare environment. The majority of the issues were recognized during the testing and validation stages, and they were corrected by making changes in the configuration. This helped in developing a more reliable and secure infrastructure.

Though the concerns did affect the overall goal of the system, they highlighted important aspects to keep in mind when carrying out medical workloads within a cloud infrastructure. The above table illustrates the most prominent challenges identified, their implications, and the strategies used to overcome them.

Issue	Description	Solution
Restriction on network access	First, communication within subnets was blocked by the Network Security Group rules.	In order to allow specifically service-to-service communication, the Network Security Group policies had to be reviewed and changed.

Integration with Azure Machine Learning Virtual Network (VNet)	There have been issues with the Azure Machine Learning services during the deployment of the machine learning model.	An alternative solution to this is ACI.
Limits of Storage Access	Because of strict network configurations, Blob Storage was not available during initial testing.	Networking settings were updated to allow access only from approved subnets using private access.
Lack of Monitoring and Coverage	some resources did not produce logs for Azure Monitor.	better monitoring and logging, diagnostic settings were enabled for all important resources.
Resource dependency order	Certain services failed to deploy due to unmet network dependencies.	Deployment order was adjusted to provision networking components before dependent services.
The order of dependencies on resources.	VNet network dependencies prevented several services from deploying.	In order to deliver networking components before dependent services, the deployment order was changed.

Table 7: Project Issues and Solution

Backup Plan

Because of the sensitivity, regulation importance, and business criticality involved in healthcare information, it is imperative to deploy a healthcare cloud system with a systematic backup process. In a healthcare cloud infrastructure, a backup system is not only used to ensure recovery from technical failure but also to provide protection from unintended deletion, damage, threats, and unplanned outages (Microsoft, 2023). The backup method used in this project was intended to ensure healthcare data integrity, accessibility, and compliance in an Azure healthcare platform.

The backup plan focused on automation, securing the backups, and ensuring recoverability, making it compliant with best practices in a regulated cloud environment. Automated methods of backup make it less dependent on human interaction, ensuring a steady recovery point, which is highly important when dealing with sensitive data of the healthcare sector (Microsoft, 2023). The use of Azure Backup Services helped to safeguard

the essential components of the infrastructure, including storage resources and managed services.

Azure Recovery Services made it easier to manage backups centrally, allowing the consistent application of retention policies. Centralized management policies improve visibility and auditing, which are critical in health information infrastructure (Microsoft, 2022). The backups were stored in a resilient architecture to provide redundancy in case of loss due to failure in the infrastructure or platform (Microsoft, 2024).

Retention policies were set up to support the ability to perform a point-in-time restores, allowing a return to a previously known good state. This matter is very important in the healthcare sector, as it relies upon the integrity and consistency of the data (ISO/IEC, 2022). Backup data was isolated to protect it from any form of unauthorized access or compromise.

Apart from protecting data, repositories with version control were also used for keeping configuration artifacts of infrastructure, such as deployment templates, network, and access controls. Infrastructure as Code and backups of infrastructure configurations are considered best practices to ensure quick recovery and deployment in cloud systems (Microsoft, 2023).

The infrastructure was rebuildable for future needs. Although disaster recovery with functionalities such as automatic failover between regions was not part of this project scope, the methods of backup implemented have laid a very good foundation for the future. Backup and recovery are the basis of disaster recovery in healthcare systems in the cloud and can serve as a foundation for the development of advanced solutions (Microsoft, 2024).

Future Plan and Work

Future versions of this system may include the following infrastructure improvements in addition to those above in order to increase levels of reliability and facilitate scale in the hospital context. Firstly, the introduction of multi-region redundancy in both the ‘storage’

and ‘database’ infrastructural layers would be essential in ensuring data and model result availability in the event of regional failures. The provision of automatic scaling in the machine learn compute infrastructure and App Service would be another area of significance in this future system version. This would allow the system to handle increased clinical load requirements automatically. It would be essential indeed to incorporate further improvements in this future system version in the use of the global routing feature in Azure Front Door service, enhanced security analysis through the use of the Azure Sentinel service, and finally, complete ‘Key Vault’ rotational requirements. The achievement of this would require infrastructural changes in the system that would include ‘VNet’ expansion, creation of new ‘subnets’ in the platform services infrastructure, ‘availability zone’ feature support, and additional ‘private endpoint’ support. The system’s ‘database’ layer would be modified in terms of ‘high availability’ in this future system version through replication settings support and automatic ‘failover’ script provision.

Synopsis of my experience

The project allowed gaining insight into how the cloud infrastructure enables an overall medical system and how this affects the precision and integrity of the process. The significance of subnet planning, network access, identity governance, and routing in the integration of machine learning computing power and databases in a regulated setting became clear. Knowledge in the deployment of Azure ML, troubleshooting in VNet integration, and conflicts in security rules has allowed improvements in troubleshooting techniques. The significance of monitoring in dealing with working loads that handle protected healthcare information has also been pointed out. The skill in designing topology views, deployment views, and activity views has enhanced the skill in presenting system designs. All acquired information and skill enhancement are necessary in future professional life because overall engineering in the IT business and accuracy in the healthcare industry are key.

Bahraini Perspectives

The project affirms conformity with Bahrain’s legal and cultural standards regarding the safeguarding of sensitive health information. The Personal Data Protection Law (PDPL) enforces strict controls over the collection, processing, storing, and accessing of personal

and health-related information. The assurance of confidentiality in healthcare, therefore entails the use of private VNets, secure data storage through encryption, secure access via VPN, or accessing through secure access-endpoints in the system's architectural framework (Personal Data Protection Authority, 2018). This addresses cultural perceptions in Bahrain regarding confidentiality and upholding patient dignity in healthcare delivery.

Moreover, this project aligns with the Ministry of Health's vision regarding digital health in Bahrain. The Ministry of Health's vision entails creating safe digital health systems and improving the level of healthcare services in the country (Ministry of Health, 2013). This project complies with this vision through the use of secure networks, private endpoints, secure routing methods, and encrypted blob storage in health care delivery in Bahrain. From the cultural perspective, the project has the capacity to create a positive effect if implemented appropriately. Bahraini patients are known to often ask for clear information regarding the processing of their health information.

The use of strict access controls in keeping data from the MRI system in private cloud computing systems may be able to retain the confidence of the patients and healthcare professionals. The healthcare system in Bahraini society may be able to retain the cultural values of respect for privacy and accountability in the healthcare system through this system if more healthcare professionals in Bahrain adopt this system.

Legal, Ethical, Social, and Professional Issues

The deployment of the medical imaging infrastructure in the cloud involves a number of significant legal, ethical, social, and professional factors. The system involves the processing of sensitive patient data through MRIs, hence requiring strict requirements in terms of data storage, transfer, access, and protection. It is imperative to thoroughly investigate the legal requirements and social factors in relation to the infrastructure platform deployment because failures in legal requirements and social factors may undermine the integrity of the entire process. This process involves health care.

Legal Issues

The system handles health data classified as sensitive personal data under the Personal Data Protection Law (PDPL) in Bahrain. PDPL requires lawful processing, express guarantees,

rigorous access controls, encryption, and normative auditing of all data transactions (Personal Data Protection Authority, 2018). This legal imperative affects all technical aspects of the system, from network compartmentalization in the private network to identity settings, rest and transit encryption, and securing data storage accounts. Legal adherence also covers data residency aspects and limiting access of the data in MRIs to only private network endpoints. Furthermore, in consideration of Microsoft's adherence to international healthcare regulatory requirements compatible with GDPR and ISO standards, additional legal obligations apply regarding system transparency, data minimization, and secure data processing (Microsoft, 2024). Network misconfigurations in data access controls or routing may violate these legal specifications. The legal requirements are therefore essential system background considerations.

Ethical Issues

The ethical aspects are brought about by the dependence of clinicians on the accuracy and integrity of the diagnostic pipeline. The process should be able to handle data in a confidential and secure manner with no chance of data breaches. The integrity of the diagnostic process should not be compromised in terms of routing functionality, computational power, subnet level segregation, or storage access functions. The clinical process may be delayed in the case of system failures or malperformance in routing functions, computational power, subnet level segregation, or storing data. It is essential to ascertain ethical soundness in implementing sufficient defenses and controls in terms of system visibility and proper mechanisms regarding system failure or malperformance. The key aspect regarding this matter involves confidentiality and integrity in the clinical-technology setting supported by secure communication channels through encryption, effective identity governance, and proper patient data treatment mechanisms (World Health Organization, 2021).

Social Issues

Social factors involve public confidence in the use of cloud medical systems in Bahrain and cultural values associating privacy with healthcare information. Patients and healthcare professionals expect the confidentiality of healthcare information to be observed. Secure architecture in this context would involve keeping all healthcare information in closed medical networks with information accessible only through accredited networks and being

more open about healthcare information security procedures in place. This would help in ensuring patient confidence in the healthcare system. The system would also meet the objectives of digital health in Bahrain in terms of providing secure, effective, and up-to-date health services (Ministry of Health, 2013). Moreover, the system would also support Bahrain Vision 2030 in terms of the strategic vision of ensuring effective digital infrastructure in the country (Government of Bahrain, 2008). However, there may be social perceptions regarding information communication and governance in the context of cloud computing and healthcare information privacy if not managed appropriately.

Professional Issues

Professional accountability is paramount in the implementation of this system. The system implementation and analysis should be carried out with accuracy and adherence to relevant standards. Any weakness in access control, routing, encryption, or system monitoring may undermine patient information integrity and undermine the integrity and competence of the professionals involved. Professional accountability involves adherence to best practices like those discussed in ISO 27001 guidelines that focus on secure system design and operation, change control, risk analysis and consideration, and continuous system surveillance (Microsoft, 2024). Another issue under professional accountability involves clear and effective system documentation and communication of information with clinical professionals. Any weaknesses or deviation from standards may undermine the integrity of the professionals or groups of professionals involved and may affect patient safety directly.

7. Conclusion

This thesis offers new, practical insights into the building of a secure and compliant cloud architecture for the management of machine learning services in a hospital environment, using Microsoft Azure. The results show that the confidentiality of healthcare information can be ensured at the infrastructure level through the enforcement of network segmentation, encryption, and controlled access, in addition to secure communication in on-premises and cloud settings. The results validate the assumption that the design of the infrastructure plays a critical role in the secure operation of machine learning systems in a sensitive field, such as medical imaging.

An important lesson learned is that cloud security and regulatory compliance are achieved not by individual services, but by the integrated assembly of networking, identity, encryption, and monitoring components. Another important aspect brought out by this study is the challenges faced when planning to meet the demands of security, scalability, and expenses, given the limitations of the project, in designing healthcare cloud systems.

Even with these prime objectives met, there are additional concerns that this research endeavors to identify and explore in the realms of future work. Some of these could include the pursuit of greater automation levels through the use of infrastructure as code, additional analysis of real-time monitoring and response to incidents, as well as an investigation of hybrid or multi-cloud models for comparison purposes.

From a practical perspective, the proposed infrastructure provides a reusable reference model for healthcare organizations wanting to create machine learning-ready cloud infrastructures in a responsible and secure way. Finally, the thesis argues that a properly designed cloud infrastructure can serve as a solid base for healthcare applications related to machine learning, at the same time as offering opportunities for future improvement and research within the safe medical cloud computing area.

8. References:

- Eliwa, E. H. I., Mohamed El Koshiry, A., Abd El-Hafeez, T., & Omar, A. (2024). Secure and Transparent Lung and Colon Cancer Classification Using Blockchain and Microsoft Azure. *Advances in Respiratory Medicine*, 92(5), 395-420.
<https://doi.org/10.3390/arm92050037>
- Daliya, V. K., & Ramesh, T. K. (2025). A Cloud-Based Optimized Ensemble Model for Risk Prediction of Diabetic Progression—An Azure Machine Learning Perspective. *IEEE Access*, 13, 11560–11575.
<https://doi.org/10.1109/access.2025.3528033>
- Oh, S., Cha, J., Ji, M., Kang, H., Kim, S., Heo, E., ... Yoo, S. (2015). Architecture Design of Healthcare Software-as-a-Service Platform for Cloud-Based Clinical Decision Support Service. *Healthcare Informatics Research*, 21(2), 102.
<https://doi.org/10.4258/hir.2015.21.2.102>
- Ali, O., Shrestha, A., Soar, J., & Wamba, S. F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. *International Journal of Information Management*, 43, 146–158.
<https://doi.org/10.1016/j.ijinfomgt.2018.07.009>
- Netshamutshedzi, N., Netshikweta, R., Ndogmo, J.-C., & Obagbuwa, I. C. (2025). A systematic review of the hybrid machine learning models for brain tumour segmentation and detection in medical images. *Frontiers in Artificial Intelligence*, 8.
<https://doi.org/10.3389/frai.2025.1615550>
- Akmalbek Bobomirzaevich Abdusalomov, Mukhriddin Mukhiddinov, & Taeg Keun Whangbo. (2023). Brain Tumor Detection Based on Deep Learning Approaches and Magnetic Resonance Imaging. *Cancers*, 15(16), 4172–4172.
<https://doi.org/10.3390/cancers15164172>
- Rezk, N. G., Alshathri, S., Sayed, A., Hemdan, E. E.-D., & El-Behery, H. (2025). Secure Hybrid Deep Learning for MRI-Based Brain Tumor Detection in Smart Medical IoT Systems. *Diagnostics*, 15(5), 639. <https://doi.org/10.3390/diagnostics15050639>
- Ahamed, Md. F., Hossain, Md. M., Nahiduzzaman, Md., Islam, Md. R., Islam, Md. R., Ahsan, M., & Haider, J. (2023). A review on brain tumor segmentation based on deep learning methods with federated learning techniques. *Computerized Medical*

Imaging and Graphics, 110, 102313.

<https://doi.org/10.1016/j.compmedimag.2023.102313>

Hannan, M. A. (2025). A Cloud-Based Approach to Brain Tumor Classification Using Convolutional Neural Networks. Theseus.fi.

<https://www.theseus.fi/handle/10024/882850>

QMENTA. (2025). Retrieved November 19, 2025, from QMENTA website:
<https://www.qmenta.com/>

Government of Bahrain. (2016). Digital Health Integration. Retrieved November 19, 2025, from Bahrain.bh website:

https://www.bahrain.bh/wps/portal/en/BNP/BahrainAtAGlance/DigitalHealthIntegration/_ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfljo8ziDT1NDTwsnA0MPMxCjAzMHN3NjQMCXA0NvEz0w1EVGlaEGhgEhnk6Bvm7uRgamBjqR6Ho9wtwMTDz97AwNzJ3Mvb3MoLqN8ABHA2I049HQRR-94fpR-IHFZdgmIOhMAq_M8NB5uAJCW8DAgpAQUXIkuDUPP2C3NDQ0LxK3ewgC0cAJsD36w!!/dz/d5/L3dHQSEvUUt3RS9nQSEh/?st=&uri=nm%3Aoid%3AZ6_1I50H8C00H6T206AG73PPE10J4

PR Newswire. (2025, November 19). GCC Smart Cities & Digital Transformation Market Surges Toward USD 907.12 Billion by 2032 as AI, 5G, and Megacity Investments Accelerate Regional Innovation | According to DataM Intelligence. Retrieved November 19, 2025, from Prnewswire.com website:

<https://www.prnewswire.com/news-releases/gcc-smart-cities--digital-transformation-market-surges-toward-usd-907-12-billion-by-2032-as-ai-5g-and-megacity-investments-accelerate-regional-innovation--according-to-datam-intelligence-302620135.html>

Dubie Dubendorfer. (2024, December 16). AWS vs Azure vs Google: Cloud Services Comparison. Retrieved November 22, 2025, from Varonis.com website:

<https://www.varonis.com/blog/aws-vs-azure-vs-google>

Amazon Web Services. (2025, November 19). what-is-aws. Retrieved November 22, 2025, from Amazon Web Services, Inc. website: <https://aws.amazon.com/what-is-aws/>

Google Cloud. (2025). Cloud Healthcare API. Retrieved November 22, 2025, from Google Cloud website: <https://cloud.google.com/healthcare-api>

Al Khalifa, H. M. S. H. B. I., Al Khalifa, H. H. S. K. B. S., Al Khalifa, H. H. S. S. B. H., & Ministry of Health. (2003). Information and Communication Technology Strategy. https://www.moh.gov.bh/Content/Files/Publications/X_102201314352.pdf

Bahrain 2030. (2023). Retrieved December 3, 2025, from Bahrain.bh website: https://www.bahrain.bh/wps/portal/en/BNP/BahrainAtAGlance/Bahrain2030!/ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8ziDT1NDTwsnA0MPPwCXAzM_D0szI3MnYz9XY_31w1EVGIaEGhgEhnk6Bvm7uRgamBjqR-HR72UE1W-AAzgaEKcfj4Io_O4P04_SjyouIWAOUGEUfmeGg8zBExLeBgQUgIKKkCXBqXn6BbmhoaF5lbrZQRaOAGtlr3w!/dz/d5/L3dHQSEvUUt3RS9nQSEh/?st=&uri=nm%3Aoid%3AZ6_1I50H8C00HNPD06OH8727B3OE3

Bahrain Economic Vision 2030. (2019). Retrieved December 3, 2025, from Ministry of Finance and National Economy website: <https://www.mofne.gov.bh/en/project-initiatives/bahrain-economic-vision-2030/>

Ersoy, A. (2022, March 23). Cloud migration for medical imaging data using Azure Health Data Services and IMS | Microsoft Azure Blog. Retrieved December 3, 2025, from Microsoft Azure Blog website: <https://azure.microsoft.com/en-us/blog/cloud-migration-for-medical-imaging-data-using-azure-health-data-services-and-ims/>

INTERNATIONAL STANDARD ISO/IEC 27001. (2013). Information technology -Security techniques -Information security management systems - Requirements Technologies de l'information -Techniques de sécurité -Systèmes de management de la sécurité de l'information -Exigences. Retrieved from <https://amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027001-2013.pdf>

lisdanielsoto. (2025, November 19). Overview of Microsoft for Healthcare reference architectures - Microsoft for Healthcare reference architecture. Retrieved December 3, 2025, from Microsoft.com website: <https://learn.microsoft.com/en-us/industry/healthcare/architecture/overview>

Microsoft. (2022, March 11). Ep 53. Retrieved December 3, 2025, from Microsoft.com website: <https://learn.microsoft.com/en-us/shows/ai-show/medical-imaging-with-azure-machine-learning>

Microsoft. (2023, October 10). Introduction to Blob (object) Storage - Azure Storage. Retrieved December 3, 2025, from Microsoft.com website:

<https://learn.microsoft.com/azure/storage/blobs/storage-blobs-introduction>

Microsoft. (2023, November 17). Introduction to Azure Queue Storage - Azure Storage. Retrieved December 3, 2025, from Microsoft.com website:

<https://learn.microsoft.com/azure/storage/queues/storage-queues-introduction>

Microsoft. (2025). About Azure VPN Gateway. Retrieved December 3, 2025, from learn.microsoft.com website: [https://learn.microsoft.com/en-us/azure/vpn-gateway/about-vpngateways](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways)

Microsoft. (2025). Azure Database for PostgreSQL documentation. Retrieved December 3, 2025, from learn.microsoft.com website: <https://learn.microsoft.com/en-us/azure/postgresql/>

Microsoft. (2025). Azure DevTest Labs documentation. Retrieved December 3, 2025, from Microsoft.com website: <https://learn.microsoft.com/azure/devtest-labs>

Microsoft. (2025). Azure Kubernetes Service (AKS) documentation. Retrieved December 3, 2025, from Microsoft.com website: <https://learn.microsoft.com/azure/aks>

Microsoft. (2025). Azure security documentation. Retrieved December 3, 2025, from Microsoft.com website: <https://learn.microsoft.com/azure/security>

Microsoft. (2025, April 24). Overview of Azure App Service - Azure App Service. Retrieved December 3, 2025, from Microsoft.com website:

<https://learn.microsoft.com/azure/app-service/overview>

Microsoft. (2025, June 26). What is Azure Application Gateway. Retrieved December 3, 2025, from Microsoft.com website:

<https://learn.microsoft.com/azure/application-gateway/overview>

Microsoft. (2025, July 15). Azure network security groups overview. Retrieved December 3, 2025, from Microsoft.com website: <https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>

Microsoft. (2025, July 17). What is Azure Virtual Network? Retrieved December 3, 2025, from Microsoft.com website: <https://learn.microsoft.com/azure/virtual-network/virtual-networks-overview>

- Microsoft. (2025, July 29). Subnet Delegation in Azure Virtual Network. Retrieved December 3, 2025, from Microsoft.com website:
<https://learn.microsoft.com/en-us/azure/virtual-network/subnet-delegation-overview>
- Microsoft. (2025, August 13). Endpoints for inference - Azure Machine Learning. Retrieved December 3, 2025, from Microsoft.com website:
<https://learn.microsoft.com/azure/machine-learning/concept-endpoints>
- Microsoft. (2025, August 26). Azure Monitor overview - Azure Monitor. Retrieved from Microsoft.com website: <https://learn.microsoft.com/azure/azure-monitor/overview>
- Microsoft. (2025, September 10). Tutorial: Deploy a model - Azure Machine Learning. Retrieved December 3, 2025, from Microsoft.com website:
<https://learn.microsoft.com/en-us/azure/machine-learning/tutorial-deploy-model?view=azureml-api-2>
- Microsoft. (2025, September 11). Azure Kubernetes Services (AKS) Core Concepts - Azure Kubernetes Service. Retrieved December 3, 2025, from Microsoft.com website: <https://learn.microsoft.com/azure/aks/concepts-clusters-workloads>
- Microsoft. (2025, October). What is Azure Firewall? Retrieved December 3, 2025, from Microsoft.com website: <https://learn.microsoft.com/azure/firewall/overview>
- Microsoft. (2025, November 10). Introduction to Azure Web Application Firewall. Retrieved December 3, 2025, from Microsoft.com website:
<https://learn.microsoft.com/azure/web-application-firewall/overview>
- Microsoft. (2025, November 10). What is Azure Backup? - Azure Backup. Retrieved December 3, 2025, from Microsoft.com website:
<https://learn.microsoft.com/azure/backup/backup-overview>
- Microsoft. (2025, November 10). What is Azure Backup? - Azure Backup. Retrieved December 18, 2025, from Microsoft.com website:
<https://learn.microsoft.com/en-us/azure/backup/backup-overview>
- Microsoft. (2025t, November 24). About Azure Bastion. Retrieved December 3, 2025, from Microsoft.com website: <https://learn.microsoft.com/azure/bastion/bastion-overview>

Microsoft. (2025, November 26). Guidance and best practices - Azure Backup. Retrieved December 18, 2025, from Microsoft.com website:
<https://learn.microsoft.com/en-us/azure/backup/guidance-best-practices>

We, H., Bin, I., & Al Khalifa. (n.d.). Law No. (30) of 2018 with Respect to Personal Data Protection Law. Retrieved from
<https://www.pdp.gov.bh/en/assets/pdf/regulations.pdf>

9. Appendices

Appendix I: System and User Manuals

User Manual

Purpose and Intended Users

The present User Manual describes how users access the cloud infrastructure created for the Brain Tumor Analysis System. The text focuses on access mechanisms and infrastructure usage, and it highlights how the infrastructure is used rather than applications or the clinical workflow.

The guide is intended for:

- Authorized Hospital Information Technology Personnel
- Project Evaluators and Supervisors

A basic understanding of cloud technology and security is assumed of the user.

System Overview for Users

The system is hosted on Microsoft Azure and aims to facilitate the secure storage, processing, and analysis of medical image data.

To the user, the infrastructure gives:

- Safe access to cloud resources.
- Isolation of internal services.
- Transfer of encrypted data.
- Centralized monitoring and visibility.
- Private network boundaries in which all necessary services are functioning.

Network Access

Users cannot directly connect to internal services via the public internet.

Key controls are:

- Internal services run inside private subnets.
- Access to the backend is restricted from the public, limited only to the frontend tier.
- The connectivity service provided is through a Site-to-Site VPN.

Before engaging with any internal resource, the user must first check that secure connectivity is enabled.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes tabs for 'My role', 'vpngw', 'Home', 'Compute', 'frontier', 'Oracle', 'FastAPI', and a 'Relaunch to update' button. Below the navigation bar, there are several browser-like tabs: 'GOOGLE AI', 'DCM', 'ECOM', 'CLOUD', 'WORDPRESS', 'YouTube', 'Bahrain Polytechnic...', 'Self Service Banner', and 'All Bookmarks'. The main title bar says 'Microsoft Azure' and 'vpngw-cloud | Connections'. The left sidebar has a tree view with nodes like 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Resource visualizer', 'Settings' (expanded), 'Configuration' (selected), and 'Connections' (selected). Under 'Connections', there are sub-options: 'Point-to-site configuration', 'Maintenance', 'Properties', and 'Locks'. The main content area displays a table titled 'Search connections' with one row: 'Name: conn-cloud-to-onprem, Status: Connected, Connection type: Site-to-site (IPsec), Peer: Ing-onprem'. At the bottom of the content area, there is a note: 'Add or remove favorites by pressing Ctrl+Shift+F'.

Figure 36: VPNgw-Cloud Connection to on Premises

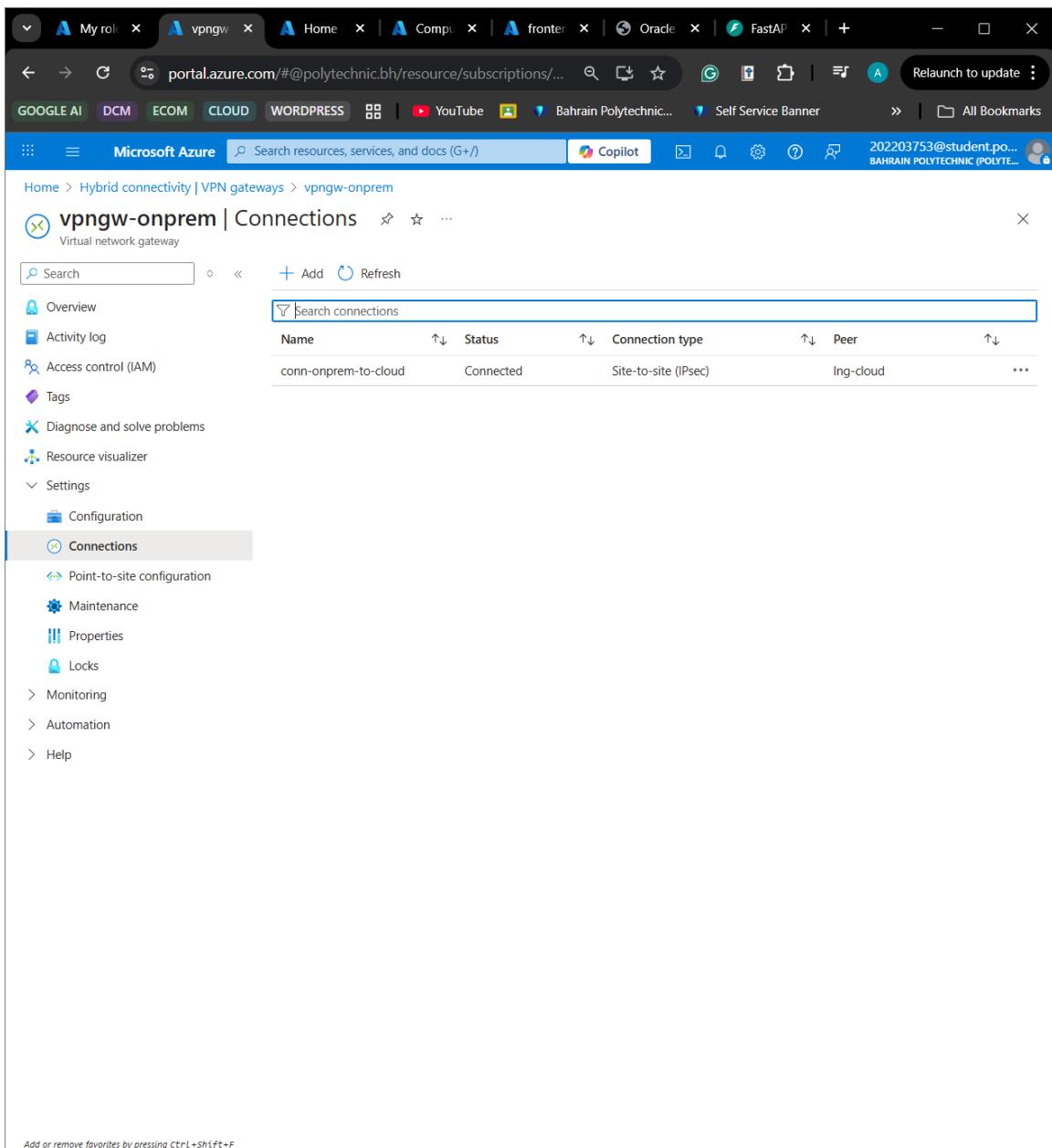


Figure 37: VPNgw- Onprem connection to cloud Cloud Services Resources

Users may:

- Check the status of virtual machines.
- Monitor the availability of resources.
- Examine the configuration summaries.

Users are prohibited from:

- Changing System Configurations.
- Start or stop production resources.
- Change network or security settings.

The screenshot shows the Microsoft Azure Compute infrastructure Virtual Machine Scale Set (VMSS) status page. The URL is https://portal.azure.com/#view/Microsoft_Azure_ComputeHub/ComputeHubMenuBlade/~/vms. The page title is "Compute infrastructure | Virtual Machine Scale Set (VMSS)". The left sidebar shows navigation options like Overview, All resources, Infrastructure, Virtual machines, Virtual Machine Scale Set (VMSS), Compute Fleet, Disks + images, Capacity + placement, Related services, Monitoring + Policy, and Help. The main content area displays a table for the VMSS named "ManagementVMSS". The table columns include Name, Subscription, Resource Group, Location, Provisioning st..., Status, and Operating syst... The status for "ManagementVMSS" is listed as Succeeded, All succeeded, Windows. There are filters at the top: Subscription equals 202203753_project, Resource Group equals all, Location equals all, and a "Give feedback" button at the bottom right.

Figure 38: VMSS Status

Name	Subscription	Resource Group	Location	Status	Operating syst...	Size	Public IP addr...	Disks
ManagementVMSS_24283443	20203753_pro...	Management-RS	West Europe	Stopped (deall...	Windows	Standard_D2s_v3	172.205.208.39	1
ManagementVMSS_b49f484f	20203753_pro...	Management-RS	West Europe	Stopped (deall...	Windows	Standard_D2s_v3	132.164.73.52	1
Onprem	20203753_pro...	Management-RS	West Europe	Stopped (deall...	Windows	Standard_D2s_v3	20.56.136.89	1
Test-Server	20203753_pro...	Management-RS	West Europe	Stopped (deall...	Windows	Standard_D2s_v3	20.224.43.129	1

Figure 39: Virtual Machines Status

Monitoring System health

It is expected that users will check the metrics of the system and notify any abnormalities.

The perspectives offered for monitoring include:

- Summary of Log Analytics
- Activity Logs

The screenshot shows the Microsoft Azure Monitor Activity log page. The left sidebar navigation includes: Overview, Activity log (selected), Alerts, Issues (preview), Metrics, Logs, Change Analysis, Service health, Workbooks, Dashboards with Grafana, Insights, Managed Services (Managed Prometheus, Azure Managed Grafana, Azure Monitor SCOM managed instance), Settings, and Support + Troubleshooting. The main content area displays a table of activity logs:

Action	Status	Time	Details	Performer
Create or Update Container App	Succeeded	4 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
List Container App Secrets	Succeeded	4 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
List Container Registry Login Credentials	Succeeded	4 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
List Container Registry Login Credentials	Succeeded	4 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
List Container Registry Login Credentials	Succeeded	4 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
List Container Registry Login Credentials	Succeeded	4 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
List Container Registry Login Credentials	Succeeded	4 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
List Container Registry Login Credentials	Succeeded	4 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
List Container Registry Login Credentials	Succeeded	4 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
Create or Update Container Registry	Failed	4 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
Creates or updates an Azure Firewall	Succeeded	5 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
Create or Update Firewall Policy Rule Collection Group	Succeeded	5 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
Creates or updates an Azure Firewall	Succeeded	5 hours ago	Sat Dec 27 ... 202203753_project	NFV Resource Provider
Creates or updates an Azure Firewall	Failed	5 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
Validate	Succeeded	5 hours ago	Sat Dec 27 ... 202203753_project	Azure Traffic Manager an...
Create or Update Firewall Policy Rule Collection Group	Accepted	5 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
Create or Update Firewall Policy Rule Collection Group	Succeeded	5 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
Creates or updates an Azure Firewall	Succeeded	5 hours ago	Sat Dec 27 ... 202203753_project	NFV Resource Provider
Validate	Succeeded	5 hours ago	Sat Dec 27 ... 202203753_project	Azure Traffic Manager an...
Create or Update Virtual Network Subnet	Succeeded	5 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
Create or Update Route	Succeeded	5 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
Auth Token for Container App Dev APIs	Succeeded	5 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
Creates or updates an Azure Firewall	Succeeded	5 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
UpdateReferences	Succeeded	5 hours ago	Sat Dec 27 ... 202203753_project	Azure Traffic Manager an...
Validate	Succeeded	5 hours ago	Sat Dec 27 ... 202203753_project	Azure Traffic Manager an...
Validate Deployment	Succeeded	5 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
Validate Deployment	Succeeded	5 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
Delete Azure Firewall	Succeeded	6 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
Auth Token for Container App Dev APIs	Succeeded	6 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
Auth Token for Container App Dev APIs	Succeeded	6 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
Create or Update Public Ip Address	Succeeded	6 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
Gets IP prefixes learned by Azure Firewall to not perform S	Accepted	6 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
Creates or updates an Azure Firewall	Failed	6 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
Creates or updates an Azure Firewall	Succeeded	6 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
Delete Public Ip Address	Succeeded	6 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
Create or Update Public Ip Address	Succeeded	6 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...
Create or Update Public Ip Address	Succeeded	6 hours ago	Sat Dec 27 ... 202203753_project	202203753@student.poly...

Figure 40: Activity logs

Limitations on User Interaction

- There is no direct way to access the databases.
- No privileges for modifying infrastructure.
- Avoid exposing publicly offered endpoints.
- These are imposed as system security and compliance measures.

User Manual Summary

Cloud infrastructure supporting the Brain Tumor Analysis System can be securely accessed and monitored by authorized users. This cloud infrastructure provides the means to ensure the safe and secure running of the healthcare tasks enabled with security and encryption.

System Manual

Purpose and Responsibilities

This System Administrator Manual contains all information pertaining to the management, maintenance, and security of the Azure cloud infrastructure supporting the Brain Tumor Analysis System. It outlines the administrative roles and procedures that are required for ensuring the availability and integrity of the proposed system.

System administrators are responsible for the following tasks:

- Azure resource and configuration management.
- Enforcement of security and access controls.
- Network Isolation.
- System health or performance monitoring.
- Backup and recovery management.
- Incident Responses & Failures.
- Documenting and getting approval for every administrative activity.

Network Administration

Virtual Network Management

One Virtual Network encompasses all the services, while workloads are segmented into isolated subnets:

- Web
- Backend
- Machine Learning
- Database
- Management
- Development

Direct communication among tiers is not permitted except when required.

Network Security Groups Management

Network Security Groups (NSGs) provide traffic filter policies at both the subnet level and resource level.

Administrator Duties:

- Allow only the necessary ports and protocols.

- Deny any incoming traffic that is not needed.
- Perform regular audits of NSG rules.

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑
300	RDP	3389	TCP	Any
320	SSH	22	TCP	Any
330	bastionaccess	3389	TCP	10.0.0.128
65000	AllowVnetInBound	Any	Any	VirtualNet
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoad
65500	DenyAllInBound	Any	Any	Any

Figure 41: Network Security group Test server NSG

Secure Connectivity Management Site-to-Site VPN

The Site-to-Site VPN provides secure connections between the hospital systems and Azure.
Administrative Tasks:

- VPN tunnel status monitoring
- Validate the encryption parameters
- The gateway must be highly available.

For the Site-to-Site VPN, the best service to be implemented is VPN Gateway method, which is best for secure connections over the internet

Connect on-premises and Azure resources

Create and manage a range of hybrid connectivity resources to provide universally available, secure, seamlessly integrated solutions with end-to-end visibility. [Learn more](#)

Overview

- > ExpressRoute
- > **VPN gateway** ● [Get started with hybrid connectivity](#)
- > Set up VPN Gateway
- > VPN gateways
- > VPN connections
- > Local network gateways
- > Virtual WAN

ExpressRoute

Set up ExpressRoute

Best for	Establishing private and high-throughput connections between on-premises network and Azure to enhance network performance, reliability, and security. Learn more
Encryption	For ExpressRoute: No For ExpressRoute Direct: Yes, MACsec
Connectivity	Private, direct connectivity
On-premises to cloud	Public IP (e.g. Azure resources) Virtual network
Throughput	Up to 100Gbps
Advance routing	BGP
Pricing	Pricing info

VPN Gateway

Set up VPN Gateway

Internet	Secure connections to private network over the internet to ensure privacy and encryption of data transmission. Learn more
Virtual network	Yes, IPsec encrypted
Throughput	Up to 10 Gbps
Advance routing	BGP, NAT
Pricing	Pricing info

Virtual WAN

Create

Give feedback
[Share feedback about your experience](#)

Figure 42: VPN Gateway in Hybrid Connectivity Overview

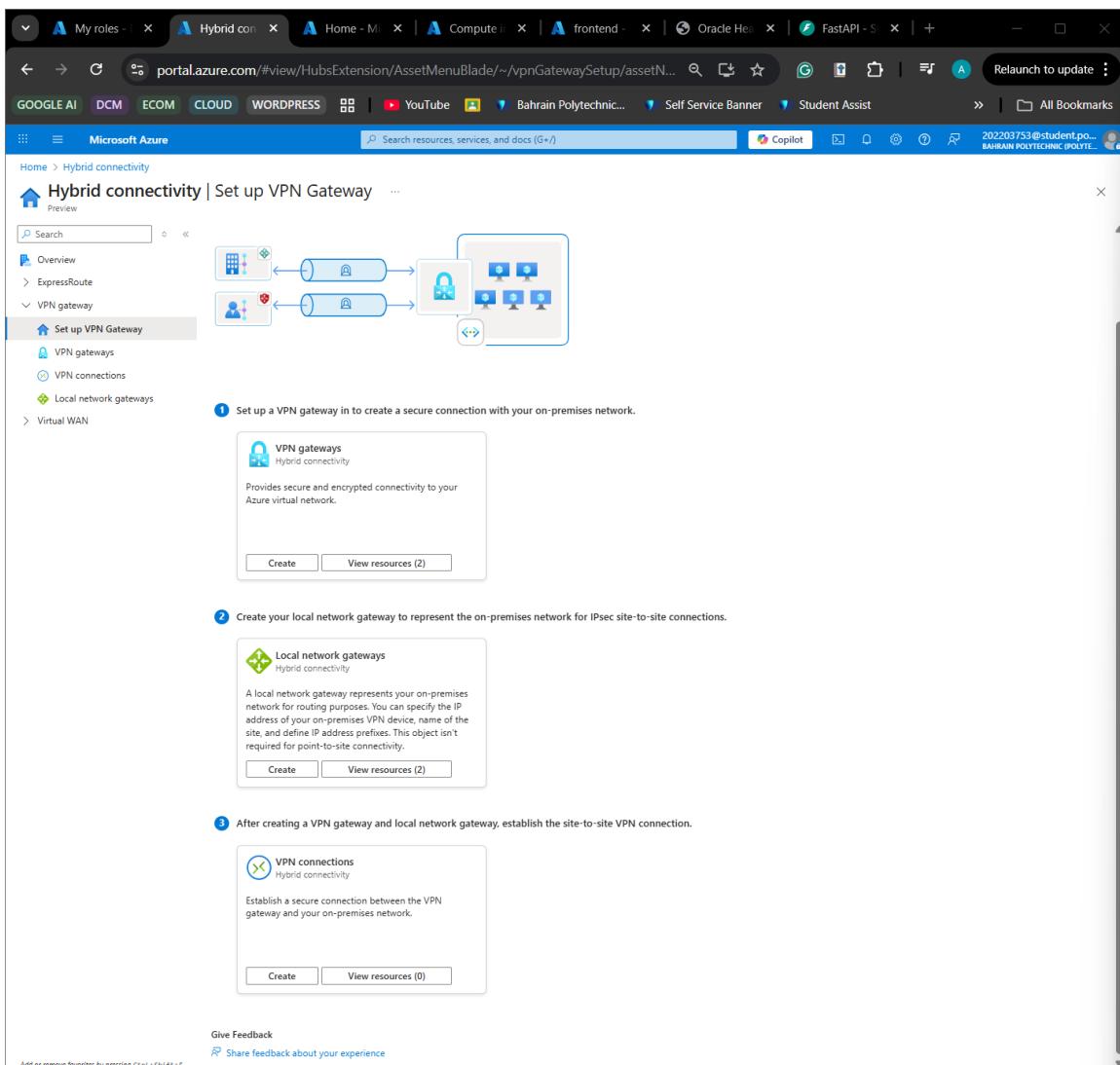


Figure 43: Recommended layout to start VPN setup

Based on Figure 43, it is recommended to start by creating VPN gateways

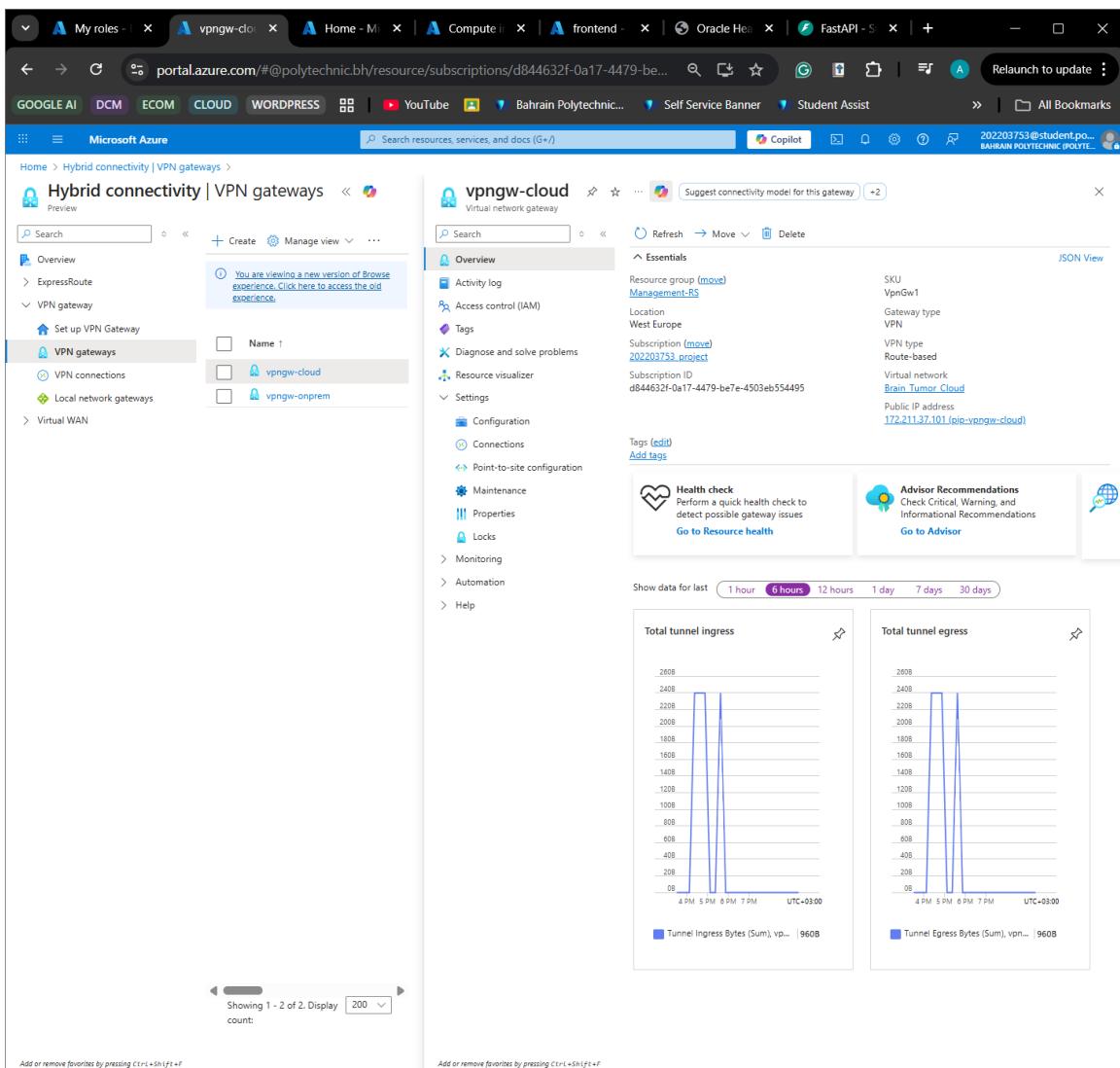


Figure 44: Site-to-Site VPN connection setup -1

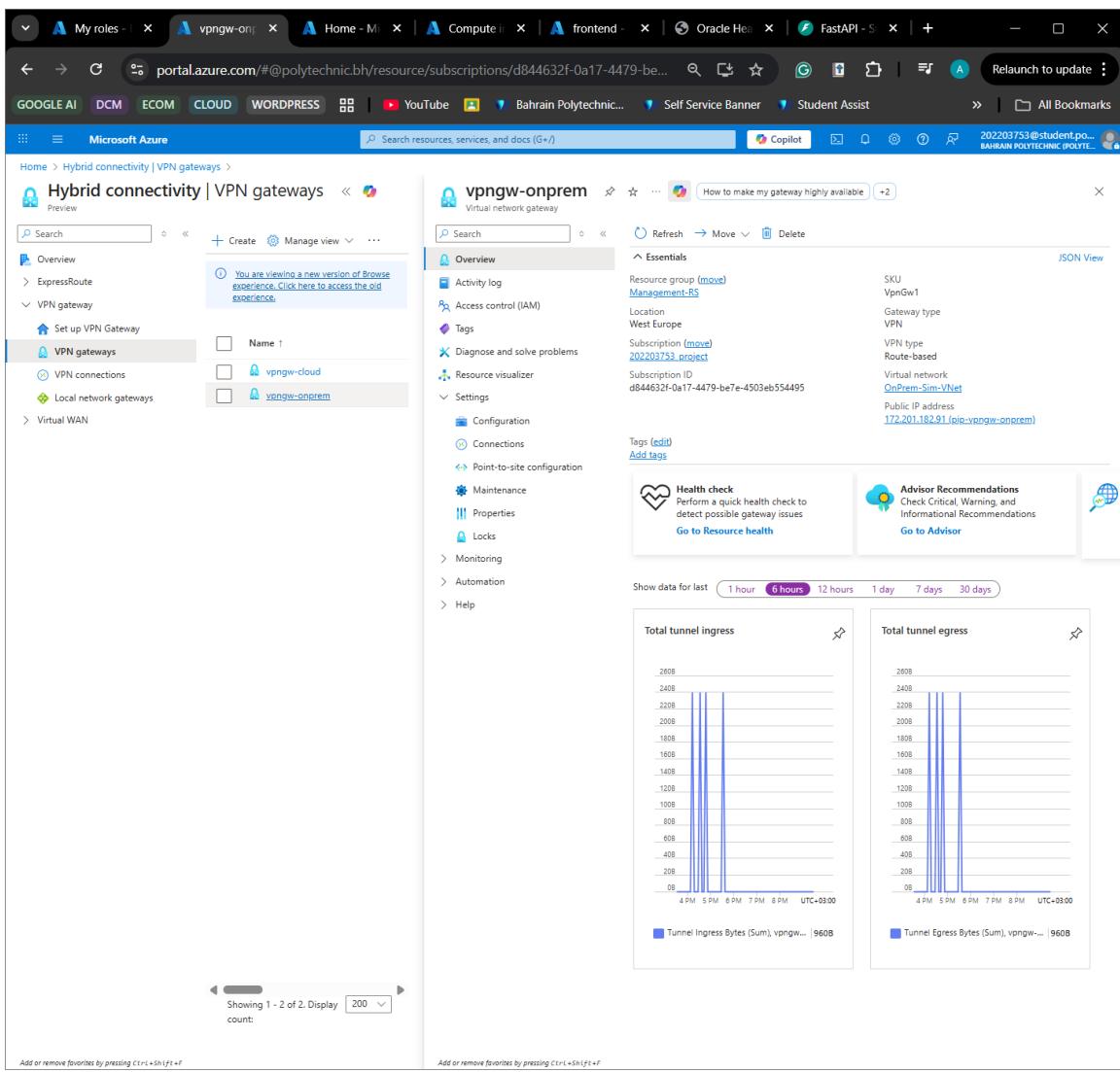


Figure 45: Site-to-Site VPN connection setup -1.1

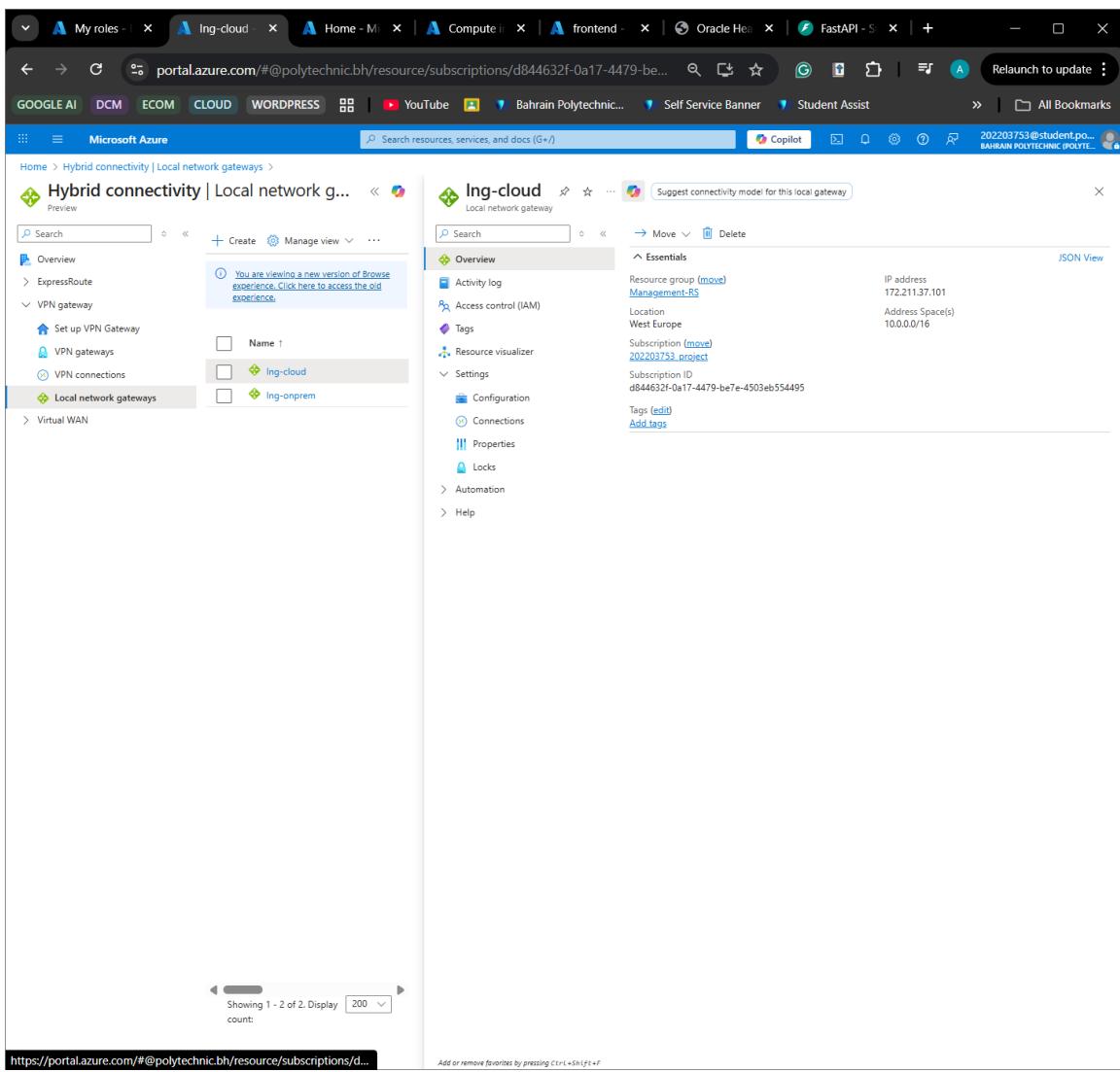


Figure 46: Site-to-Site VPN connection setup -2

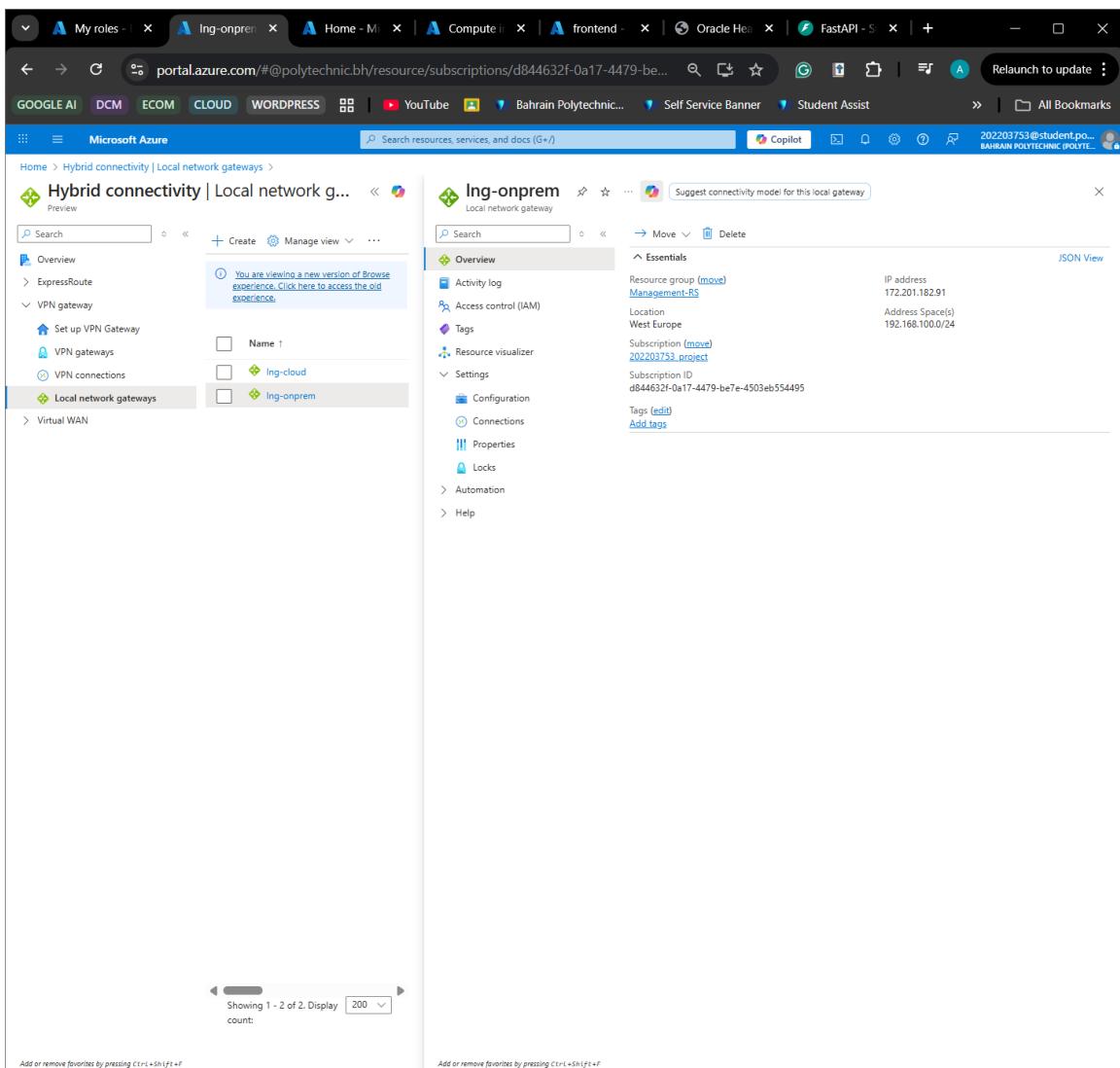


Figure 47: Site-to-Site VPN connection setup -2.1

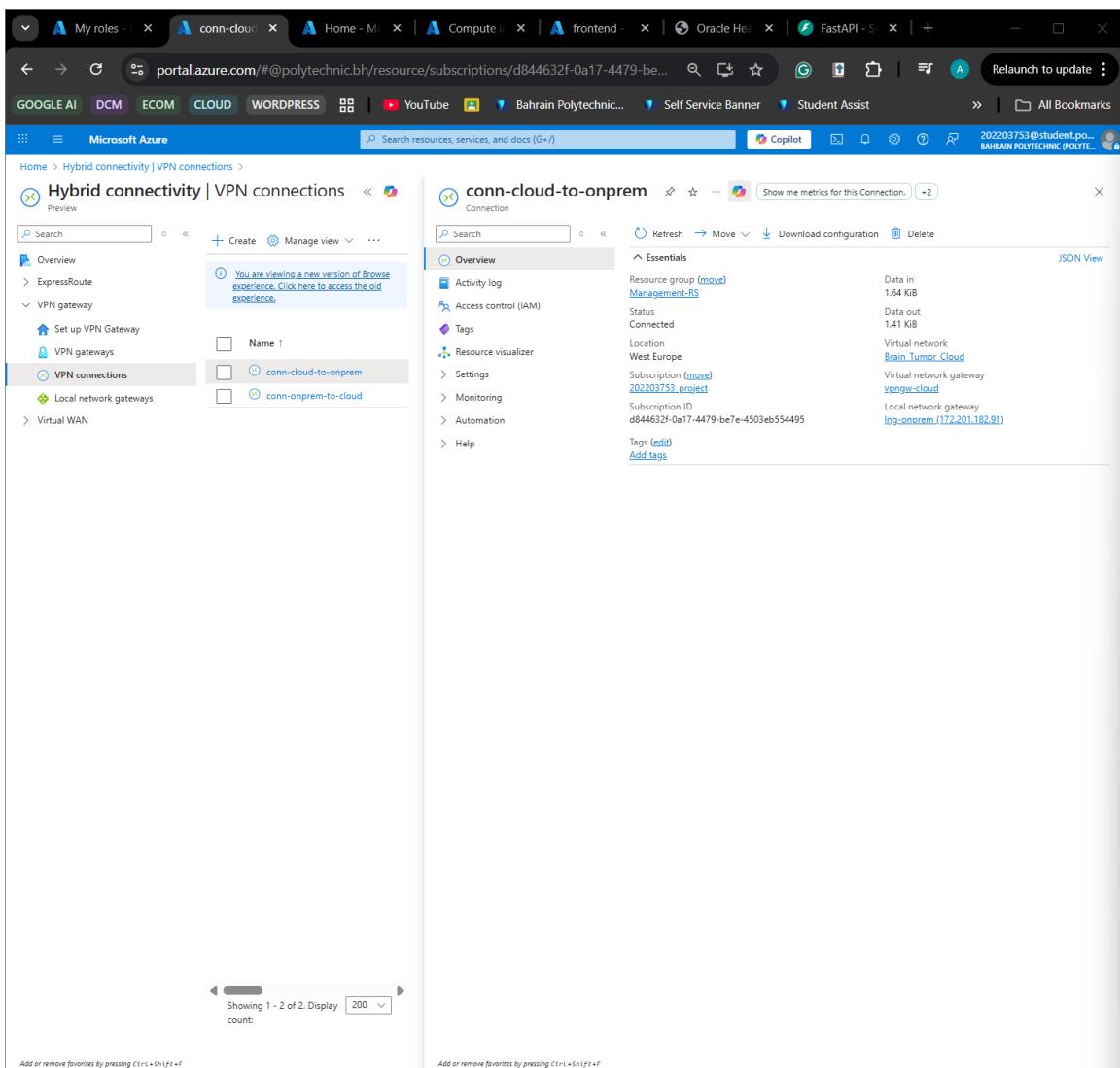


Figure 48: Site-to-Site VPN connection setup -3

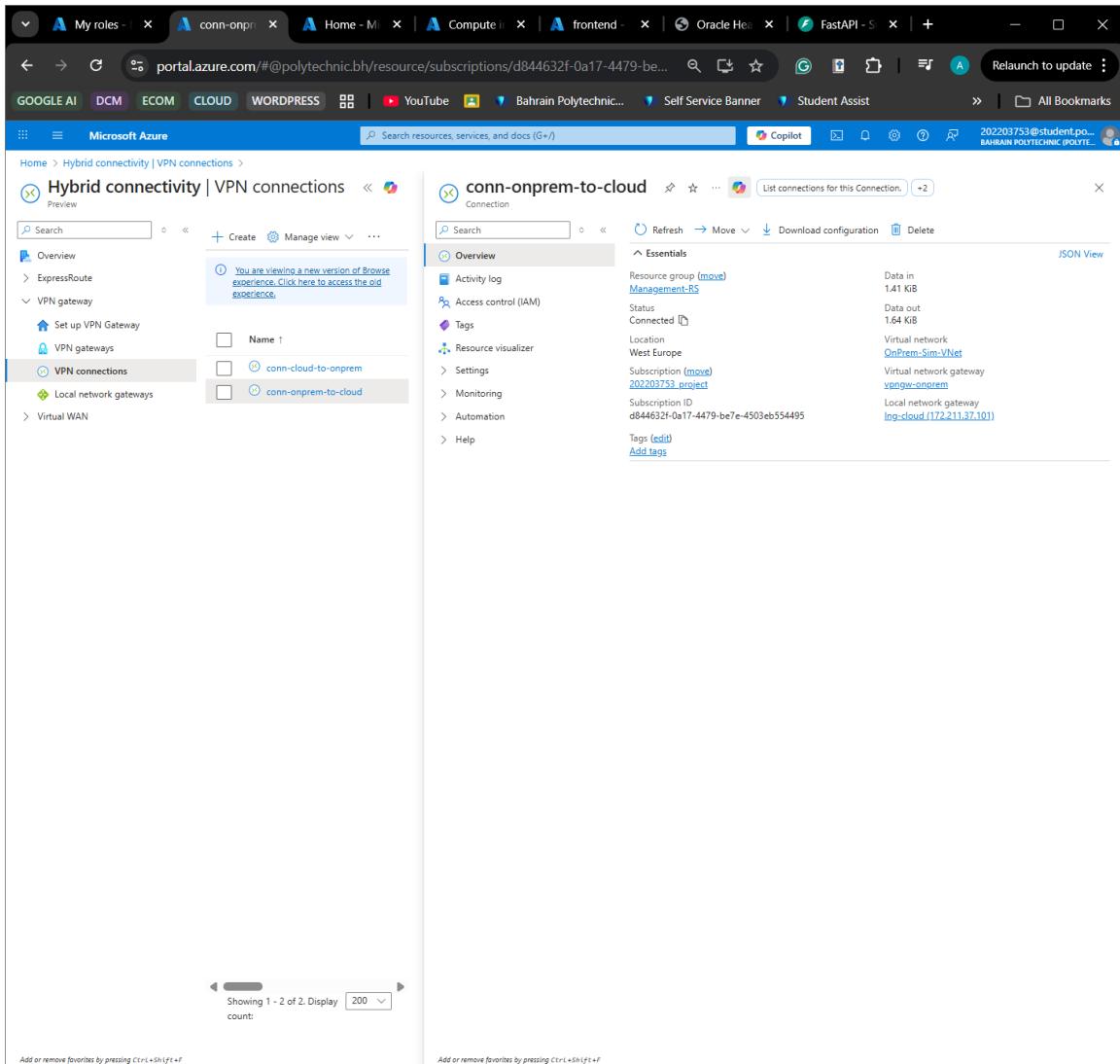


Figure 49: Site-to-Site VPN connection setup -3.1

Cloud Compute Resources

The cloud computing resources form the main processing tier of this architecture, which is delivered through Azure virtual machines and corresponding compute management services in Azure. The main function of computing resources is to offer backend processing capabilities, manage administrative operations, and execute machine learning tasks while meeting strict security needs. The compute resources run in separate subnets that do not have public accessibility, ensuring that all processing operations are conducted in a secured network environment. The size and corresponding needs-driven allocation of computing resources are used to strike a balance between processing and economical considerations.

The Azure management console gives administrators corresponding abilities to manage

compute lifecycle operations such as creation, monitoring, and maintenance, which facilitate continuous system functionality and future scalability that meets healthcare security and regulatory standards.

Virtual Machines

Administrators may:

- Provision Virtual Machines.
- Applying Updates & Patches.
- Resource utilization monitoring.

Administrators must:

- Prevent unnecessary public IP address assignments.
- Adopt security hardening practices.

The screenshot shows the Microsoft Azure Deployment Overview page for a deployment named "CreateVm-MicrosoftWindowsServer.WindowsServer-202-20251227134833". The main message is "Your deployment is complete".

Deployment details:

Resource	Type	Status	Operations
Onprem	Microsoft.Compute/virtualmachines	OK	O
onprem142_z2	Microsoft.Network/networkInterfaces	OK	O
Onprem-nsg	Microsoft.Network/networkSecurityGroups	OK	O
Onprem-ip	Microsoft.Network/publicIPAddresses	OK	O

Next steps:

- Setup auto-shutdown Recommended
- Monitor VM health, performance and network dependencies Recommended
- Run a script inside the virtual machine Recommended

[Go to resource](#) [Create another VM](#)

[Give feedback](#) [Tell us about your experience with deployment](#)

Cost Management: Get notified to stay within your budget and prevent unexpected charges on your bill. [Set up cost alerts >](#)

Microsoft Defender for Cloud: Secure your apps and infrastructure. [Go to Microsoft Defender for Cloud >](#)

Free Microsoft tutorials: [Start learning today >](#)

Work with an expert: Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support. [Find an Azure expert >](#)

Figure 50: On Premises VM deployment Complete

The screenshot shows the Azure VMSS (Virtual Machine Scale Set) dashboard for a scale set named 'ManagementVMSS'. The main pane displays the following details:

- Resource group (moved):** Management-RS
- Status:** 2 out of 2 succeeded
- Subscription:** 20200313-project
- Location (move):** West Europe
- Subscription ID:** d84463f1-0a17-4479-be7e-d503ab554495
- Tags (edit):** Add tags
- Properties:** Operating system: Windows, Capacity reservation group: -, Hibernation: Disabled.
- Azure Spot:** Azure Spot: Disabled.
- Virtual machine profile:** Virtual machine profile: Standard_DS_v2_2.
- Availability + scaling:** Availability zone: 2 (local), Extended zone: -, Proximity placement group: -, Colocation status: -, Host group: -, Instance count: 2, Scaling: Autoscale, Scale-in policy: Default, Overprovisioning: -, Fault domain count: 1, Single placement group: -, Disk controller type: SCSI.

The right side of the dashboard is divided into several sections:

- Status:** Provisioning state: Succeeded, Power state: 2 out of 2 instances running.
- Networking:** Public IP address: 172.20.208.39 (Network interface Brain_Tumor_Cloud-nic01-x15a50e1), 172.20.245.241 (Network interface ManageVMSS_NIC-1001-e54), 20.56.148.239 (Network interface ManageVMSS_NIC-x15a50e1), 123.123.123.123 (Network interface Brain_Tumor_Cloud-nic1-b001-e54). Virtual network/subnet: Brain_Tumor_Cloud/Web_App_Subnet.
- Size:** Size: Standard_DS_v2_2, vCPUs: 2, RAM: 8 GiB.
- Source image details:** Source image publisher: MicrosoftWindowsServer, Source image offer: WindowsServer, Source image plan: 2025-datacenter-Q2.
- Disk:** Disk information.

Figure 51: VMSS Dashboard

The screenshot shows the Microsoft Azure 'Create a virtual machine' interface. At the top, there's a navigation bar with 'Microsoft Azure', a search bar, and various icons. The main title is 'Create a virtual machine'. Below the title, a green banner says 'Validation passed'. There are three tabs: 'Help me create a low cost VM', 'Help me create a VM optimized for high availability', and 'Help me choose the right VM size for my workload'. The 'Review + create' tab is selected. Under 'Price', it shows '1 X Standard D2s v3 by Microsoft' and a price of '0.2353 USD/hr'. It also mentions 'Subscription credits apply' and links to 'Terms of use' and 'Privacy policy'. A section titled 'TERMS' contains legal text about agreeing to terms and conditions. A warning message in a yellow box says: '⚠ You have set RDP, SSH port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.' The 'Basics' section lists configuration details:

Subscription	202203753_project
Resource group	Management-RS
Virtual machine name	Test-Server
Region	West Europe
Availability options	Availability zone
Zone options	Self-selected zone
Availability zone	2
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Windows Server 2019 Datacenter - Gen2

At the bottom, there are buttons for '< Previous' and 'Next >', a large blue 'Create' button, and links for 'Download a template for automation' and 'Give feedback'.

Figure 52: Test Server Deployment Summary -1

The screenshot shows the Microsoft Azure 'Create a virtual machine' configuration interface. At the top, there's a navigation bar with 'Microsoft Azure', a search bar, and various account and service icons. The main title is 'Create a virtual machine'. Below the title, a green validation message says 'Validation passed'. There are three help buttons: 'Help me choose a low cost VM', 'Help me create a VM optimized for high availability', and 'Help me choose the right VM size for my workload'. The configuration is divided into several sections:

- VM settings:** VM architecture (x64), Size (Standard D2s v3 (2 vcpus, 8 GiB memory)), Enable Hibernation (No), Username (BT Dadmin), Public inbound ports (RDP, SSH), Already have a Windows license? (No), Azure Spot (No).
- Disk settings:** OS disk size (Image default), OS disk type (Standard SSD LRS), Use managed disks (Yes), Delete OS disk with VM (Enabled), Ephemeral OS disk (No).
- Networking settings:** Virtual network (Brain_Tumor_Cloud), Subnet (Development (10.0.6.0/24)), Public IP (new Test-Server-ip), Accelerated networking (On), Place this virtual machine behind an existing load balancing solution? (No), Delete public IP and NIC when VM is deleted (Enabled).
- Management settings:** Microsoft Defender for Cloud (Basic (free)), System assigned managed identity (Off), Login with Microsoft Entra ID (Off), Auto-shutdown (On), Backup (Disabled), Site Recovery (Disabled).

At the bottom, there are navigation buttons ('< Previous', 'Next >', 'Create'), a link to 'Download a template for automation', and a 'Give feedback' button.

Figure 53: Test Server Deployment Summary -2

Machine Learning Infrastructure

The Azure Machine Learning workspace was centrally maintained.

Administrator's responsibilities:

- Administer health and Status of container-related instances
- Troubleshoot problems if occurred

FastAPI 0.1.0 OAS 3.1

/openapi.json

default

GET /health Health Check

Parameters

No parameters

Try it out

Responses

Code	Description	Links
200	Successful Response	No links

Media type

application/json

Controls Accept header.

Example Value | Schema

"string"

POST /analyze Analyze

Parameters

No parameters

Cancel Reset

Request body required

application/json

Figure 54: Health of ML model

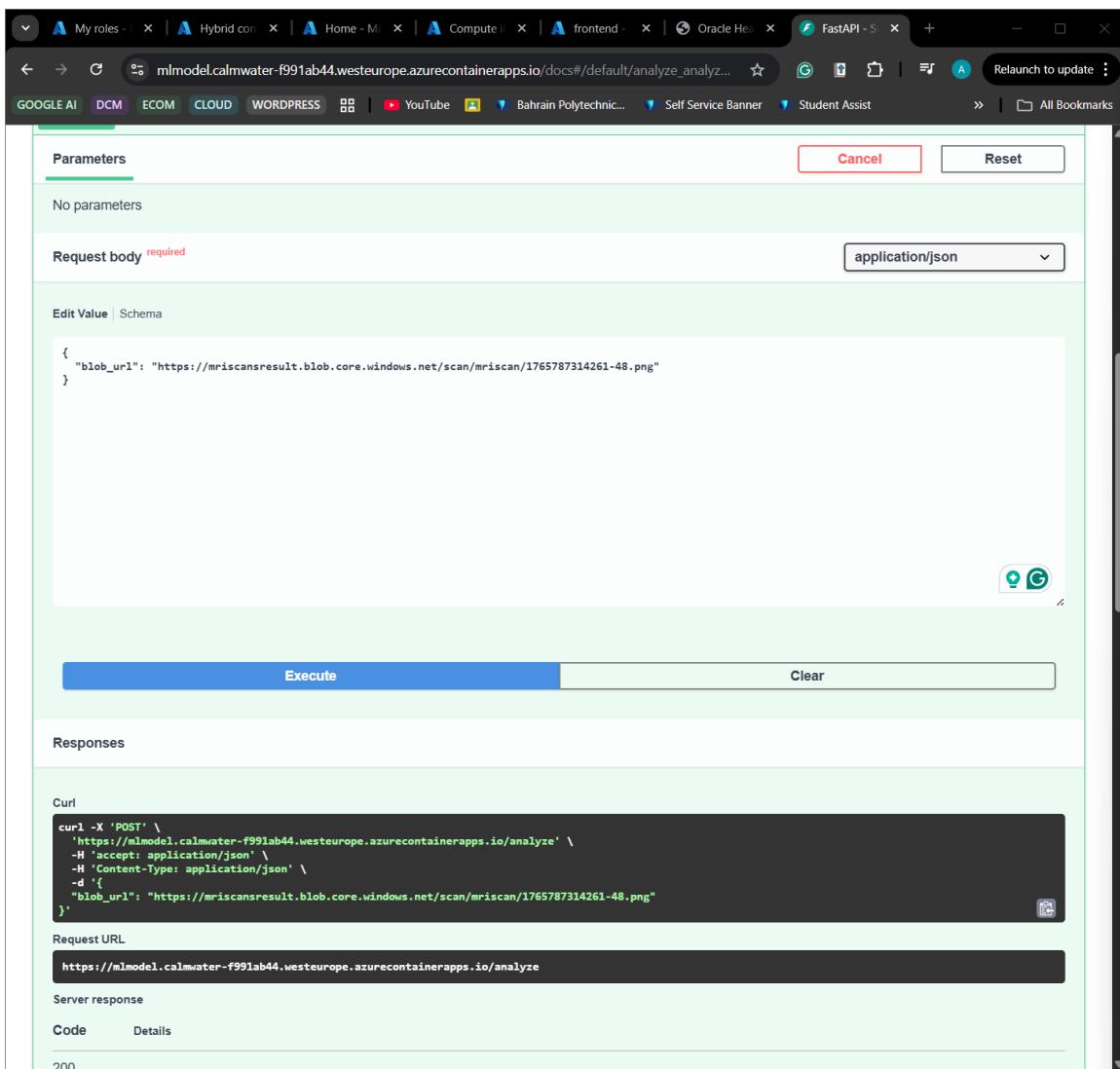


Figure 55: ML model Test Data

```

curl -X 'POST' \
  'https://mlmodel.calmwater-f991ab44.westeurope.azurecontainerapps.io/analyze' \
  -H 'accept: application/json' \
  -H 'Content-Type: application/json' \
  -d '{
    "blob_url": "https://mriscansresult.blob.core.windows.net/scan/mriscan/1765787314261-48.png"
  }'

```

Request URL
`https://mlmodel.calmwater-f991ab44.westeurope.azurecontainerapps.io/analyze`

Server response

Code	Details						
200	<p>Response body</p> <pre>{ "has_tumor": true, "confidence": 0.9999999403953552, "segmented_image_url": "https://mriscansresult.blob.core.windows.net/scan/segmentation/1765787314261-48_segmented.png", "summary": "An abnormal focal lesion has been identified on the MRI examination. The characteristics of this lesion are consistent with a neoplastic process, and its estimated size falls within the small category. Further clinical and diagnostic evaluation is recommended.", "findings": ["Presence of an abnormal focal lesion.", "Morphologic features are consistent with a neoplastic etiology.", "The lesion is categorized as small in estimated size.", "Precise location and detailed characterization require expert radiological review."], "recommendations": "Clinical correlation and further diagnostic evaluation, which may include additional imaging or biopsy, are recommended to confirm these findings and establish appropriate patient management.", "metadata": { "tumor_pixels": 5819, "tumor_percentage": 5819, "bounding_box": [151, 161, 228, 258], "centroid": [191.46124763705103, 208.97783124248153] } }</pre> <p>Response headers</p> <pre> content-length: 1165 content-type: application/json date: Wed, 24 Dec 2025 19:07:33 GMT server: uvicorn </pre> <p>Responses</p> <table border="1"> <thead> <tr> <th>Code</th> <th>Description</th> <th>Links</th> </tr> </thead> <tbody> <tr> <td>200</td> <td>Successful Response</td> <td>No links</td> </tr> </tbody> </table> <p>Media type <input type="button" value="application/json"/> <input type="button" value="text/plain"/> Controls Accept header</p>	Code	Description	Links	200	Successful Response	No links
Code	Description	Links					
200	Successful Response	No links					

Figure 56: ML Model Test Data Outcome

Monitoring and Logs

There are several Azure tools available for monitoring, which include:

- Azure Monitor
- log analytics

Responsibilities of Administrators:

- Perform reviews of log files.
- Set alert thresholds.
- Immediately examine anomalies that are detected.

System Manual Summary

This document, the System Administrator Manual, explains the operation and security duties that are ought to be in place for the management of the cloud infrastructure that underlies the Brain Tumor Analysis System. This infrastructure has the aim of being secure, reliable, and meets the regulations of cloud data security for the health sector.

Appendix II: Detailed Design

Purpose

This appendix contains a set of design diagrams that comprise the infrastructure design for the Brain Tumor Detection System on Microsoft Azure. This serves as an addition to Chapter 3 (Design), where architectural diagrams are used to describe how networking and computation resources, and other components, are structured and integrated together. These diagrams presented within this appendix are used as design evidence that supports traceability from functional requirements to design.

Architecture Design

The system has a tiered cloud architecture that runs on Azure, all encompassed in one Virtual Network. This helps to ensure segregation by specific subnets and security restrictions, which helps limit the attack surface and ensure that the communication is compliance-bound. Those features enable secure data ingestion, machine learning inference, database storage, and privileged access by administrators and medical professionals.

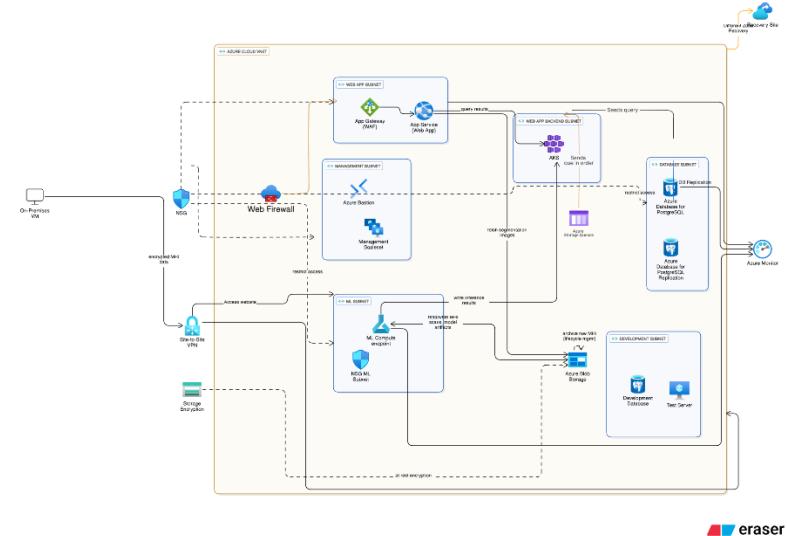


Figure 57: Azure Cloud Design

Network Design

Within a single Azure Virtual Network, all system resources are unified, providing private IP networking and centralized policy enforcement.

VNet Address Space: 10.0.0.0/16

The VNet is divided into subnets specific to their function.

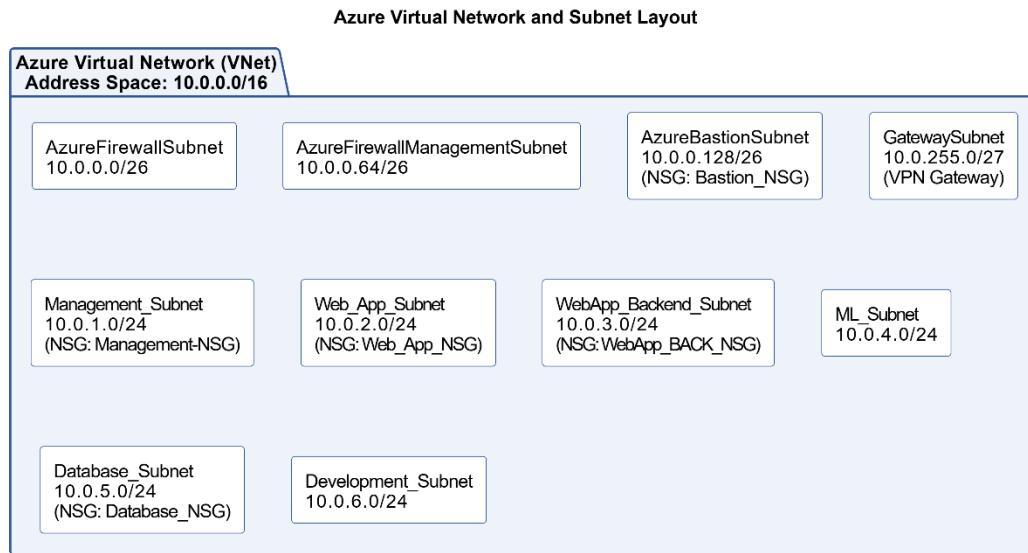


Figure 58: Subnet layout

Subnet	Purpose	Range
AzureFirewallSubnet	Azure Firewall	10.0.0.0 – 10.0.0.63 /26
AzureFirewallManagementSubnet	Management of Firewall	10.0.0.64 – 10.0.0.127 /26
AzureBastionSubnet	Secure access	10.0.0.128 – 10.0.0.191 /26
Management_Subnet	Administrative access	10.0.1.0 – 10.0.1.255 /26
Web_App_Subnet	To host the front-end and website	10.0.2.0 – 10.0.2.255 /24
WebApp_Backend_Subnet	Backend services and AKS	10.0.3.0 – 10.0.3.255 /24
ML_Subnet	To host Machine Learning modules	10.0.4.0 – 10.0.4.255 /24
Database_Subnet	Contains the Database Services for the website	10.0.5.0 – 10.0.5.255 /24
Development	Development and testing	10.0.6.0 – 10.0.6.255 /24
GatewaySubnet	Site-to-Site VPN connection	10.0.255.0/27

Table 8: IP Scheme

The approach to IP address assignment uses a single private /16 address range compatible with long-term scalability needs while maintaining logical separation among the various

system components. The subnets reserved by Azure are allocated in the form of the minimum required /26 CIDR blocks, while workloads are allocated /24 address ranges to support horizontal scaling and service expansion.

Route tables are associated with all the traffic-controlled subnets to allow centralized routing through the Azure Firewall, thus enabling zero-trust networking. Delegation of services to the database subnet is granted to allow seamless connectivity with Microsoft Azure Database for PostgreSQL. Unauthorized deployment of resources on the database subnet is prevented.

Site-to-Site VPN Design Requirements

The Site-to-Site VPN configuration that enables a safe connection between the on-premises network with the IP range 192.168.1.0/24 and the Virtual Network in Microsoft Azure with the IP range 10.0.0.0/16. A local VPN connection on the on-premises network is terminated using the on-premises VPN device/firewall with the on-premises Public IP, as opposed to a VPN Gateway device in Microsoft Azure with the name VpnGw1, which is in GatewaySubnet with IP 10.0.255.0/27. Additionally, on Microsoft Azure, the VPN

The VPN tunnel uses IKEv2 for authentication and key agreement, together with IPsec ESP for encrypting data transfer. Strong security settings are also used, such as AES-256 encryption, SHA-256 hashing, together with Diffie-Hellman Group 14. The always-on functionality of the tunnel allows for encrypted and private communication to take place between Azure internal subnets (Web, Backend, ML, and Database), as well as on-premises systems, without exposing services to the internet.

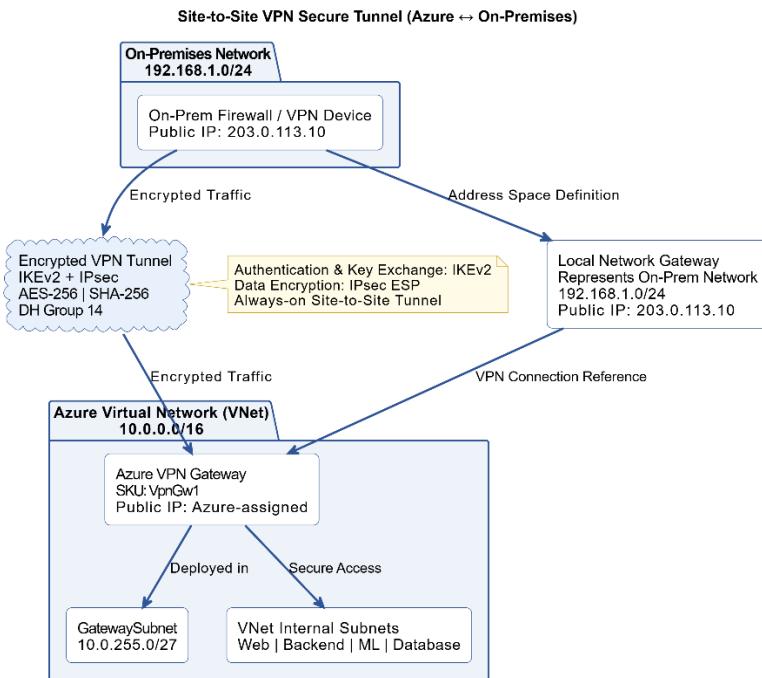


Figure 59: Site-to-Site VPN Tunnel Diagram

Cloud Compute Resources Design

Azure Container Instance (ACI) is used as the means to deliver applications as well as backend operations. Services communicate with each other on private subnets without any public IPs, which ensures secure communication.

Machine learning inference workloads run atop Azure Machine Learning compute resources hosted inside a reserved subnet.

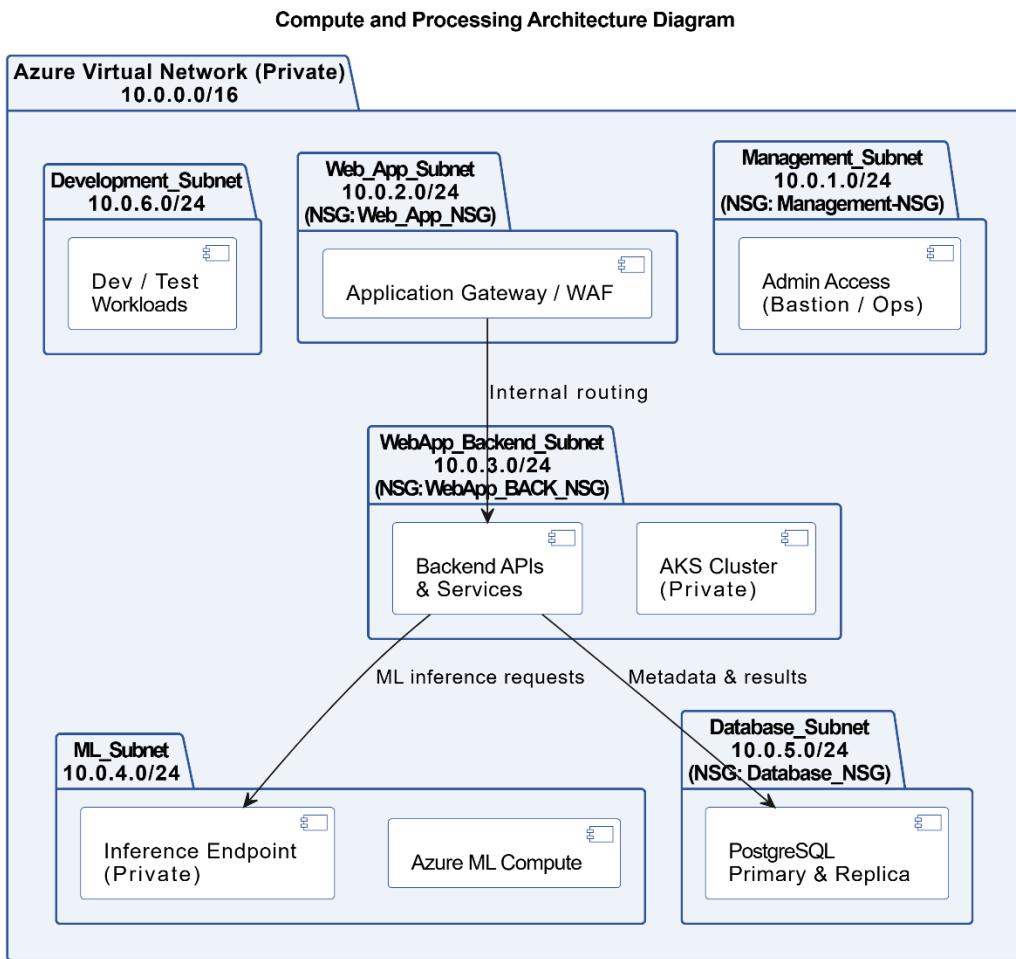


Figure 60: Compute and Processing Diagram

Data Storage and Database Design

Azure Blob Storage is used for storing MRI images and inference artifacts. PostgreSQL databases store metadata and inference results and are running inside a private subnet.

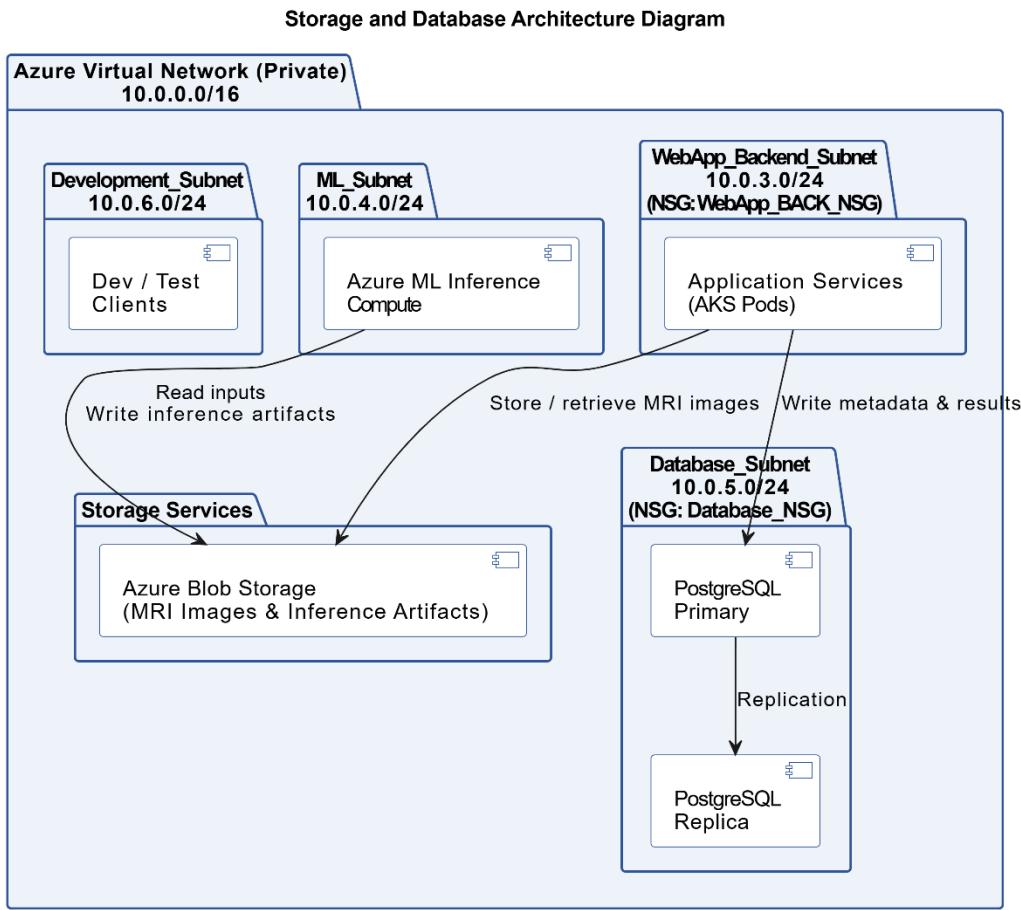


Figure 61: Storage and DB Architecture

This storage and database architecture is implemented inside the private Azure Virtual Network range of 10.0.0.0/16 in order to enable the secure processing of the MRI images and the machine learning inference. This design breaks down the environment into separate subsets for the components of the development environment, the machine learning environment, the backend environment, the storage environment, and the database environment.

Azure Blob Storage is used for storing MRI images and results of inferences because of its scalability and ability to handle large volumes of unstructured healthcare information. The database level is isolated in its own subnet and designed as PostgreSQL primary-replica topology to improve its resilience and availability. Backend application services are the sole entities that are allowed write access to metadata and results of inferences and

represent the only elements that fulfill the confidentiality, integrity, and availability constraints applicable in healthcare workloads.

Appendix IV: Detailed Implementation

Since the project is built on the cloud, there will not be a lot of coding, mostly screenshots, and there will be scripts that were generated by Azure if this project were to be recreated through the script, and most of the scripts would be found GitHub repository for the project by clicking on this [link](#).

Setting up the environment

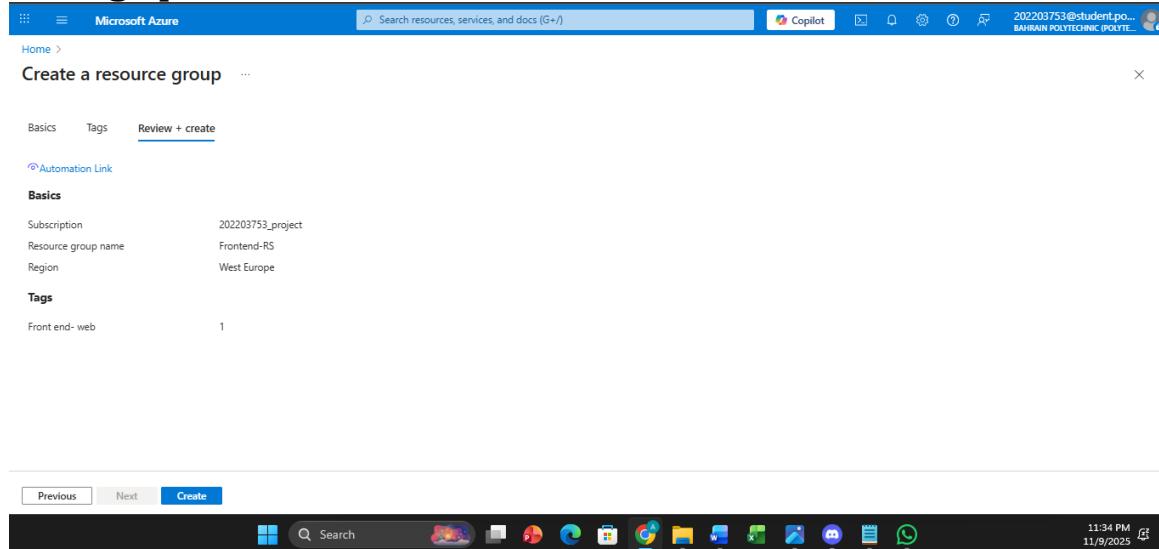


Figure 62: Resource Group Creation

Start by setting up resource groups similar to the figure shown

Name	Subscription	Location
Backend-RS	202203753_project	West Europe
Brainumor-front_group	202203753_project	West Europe
DefaultResourceGroup-WEU	202203753_project	West Europe
Frontend-RS	202203753_project	West Europe
MA_defaultazuremonitorworkspace-weu_westeurope_managed	202203753_project	West Europe
Management-RS	202203753_project	West Europe
ME_backend-env_backend-rs_westeurope	202203753_project	West Europe
ML-RS	202203753_project	West Europe
NetworkWatcherRG	202203753_project	West Europe
Security-RS	202203753_project	West Europe

Figure 63: Resource groups Tab

Afterwards, Set up the Virtual Network like the figures below, or use Azure CLI to create them automatically.

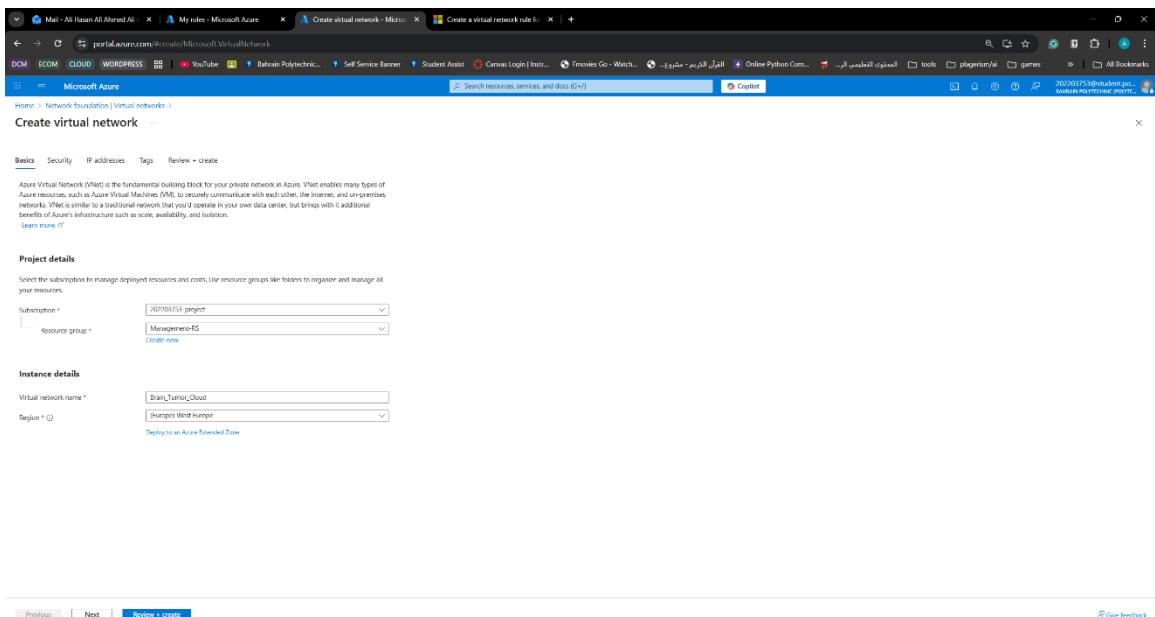


Figure 64: Vnet Creation pt-1

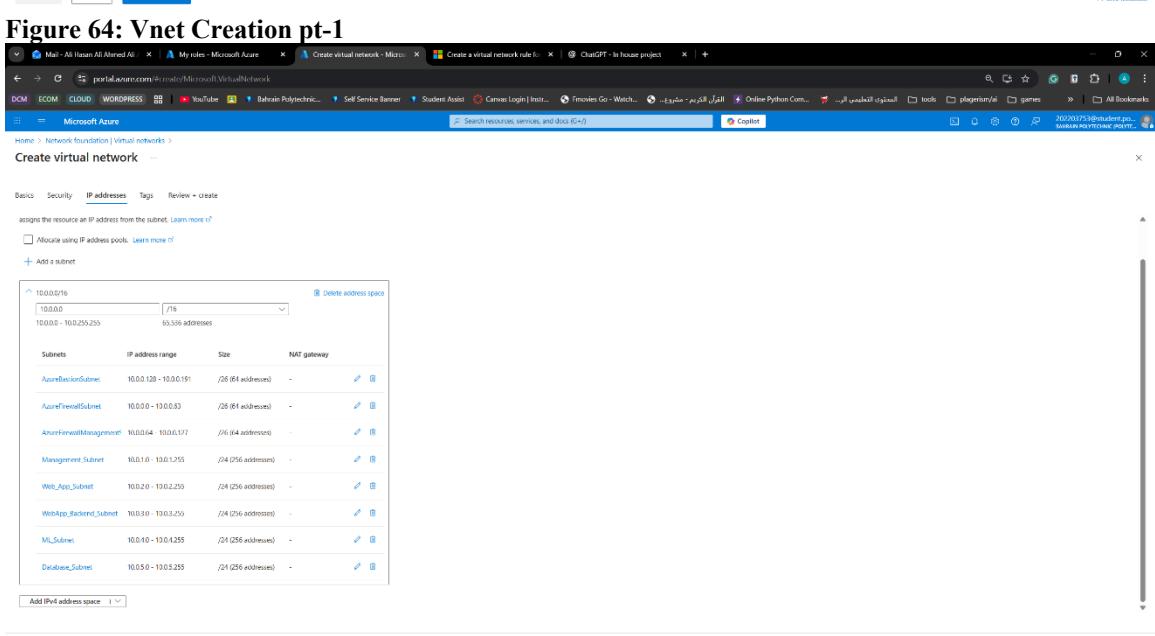


Figure 65: Vnet Creation pt-2

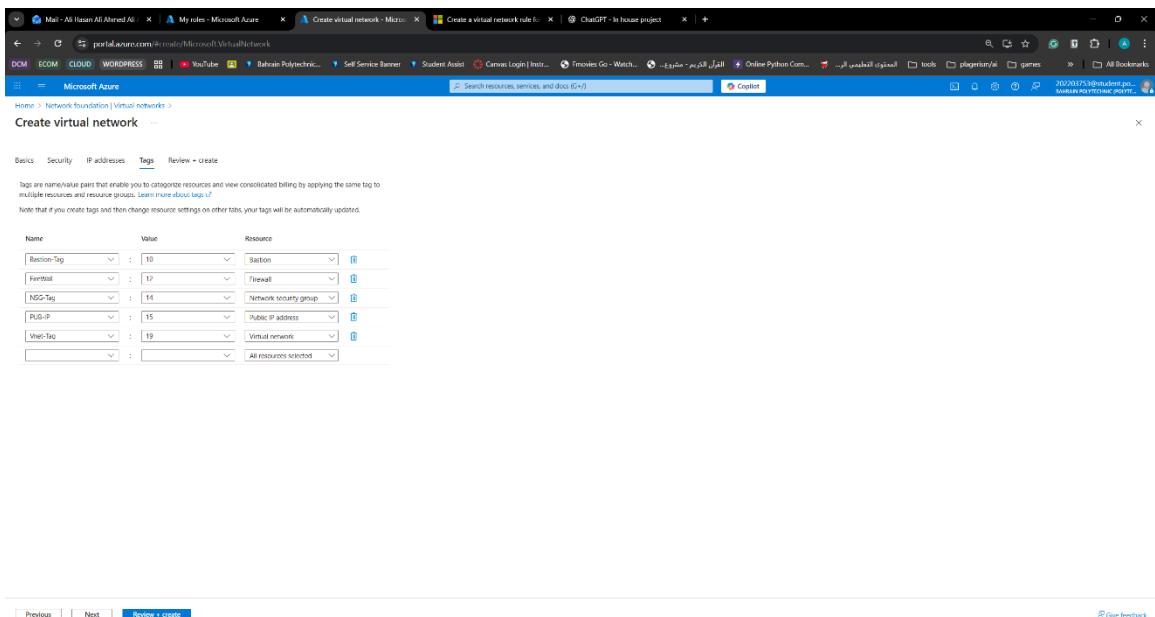


Figure 66: Vnet Creation pt-3

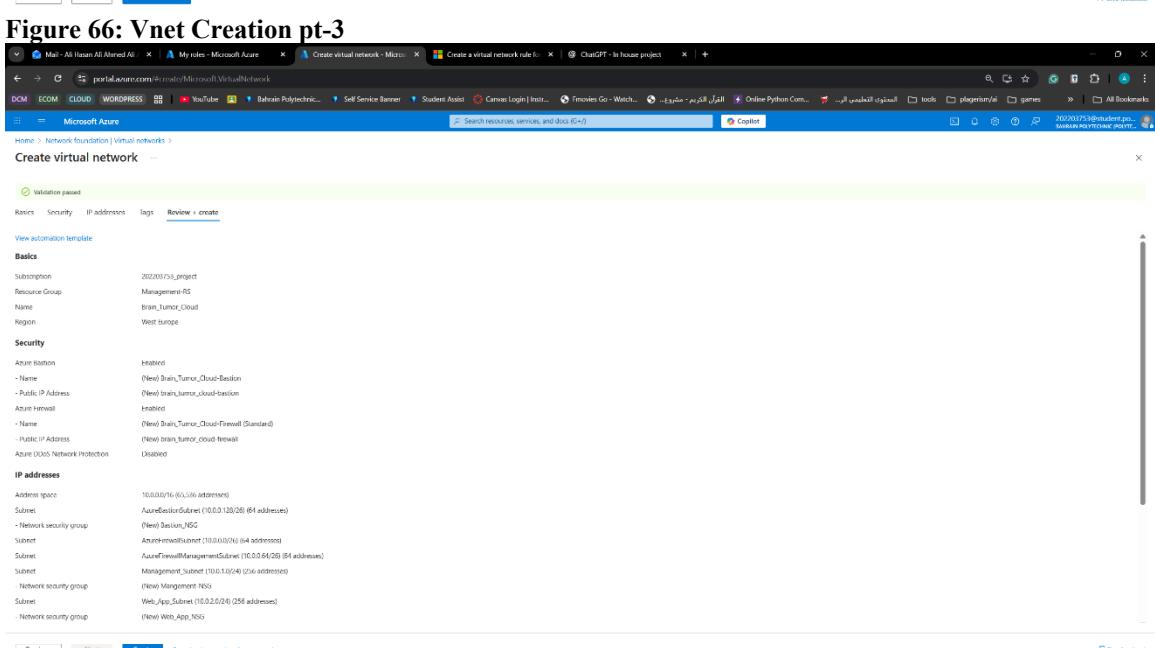


Figure 67: Vnet Creation pt-4

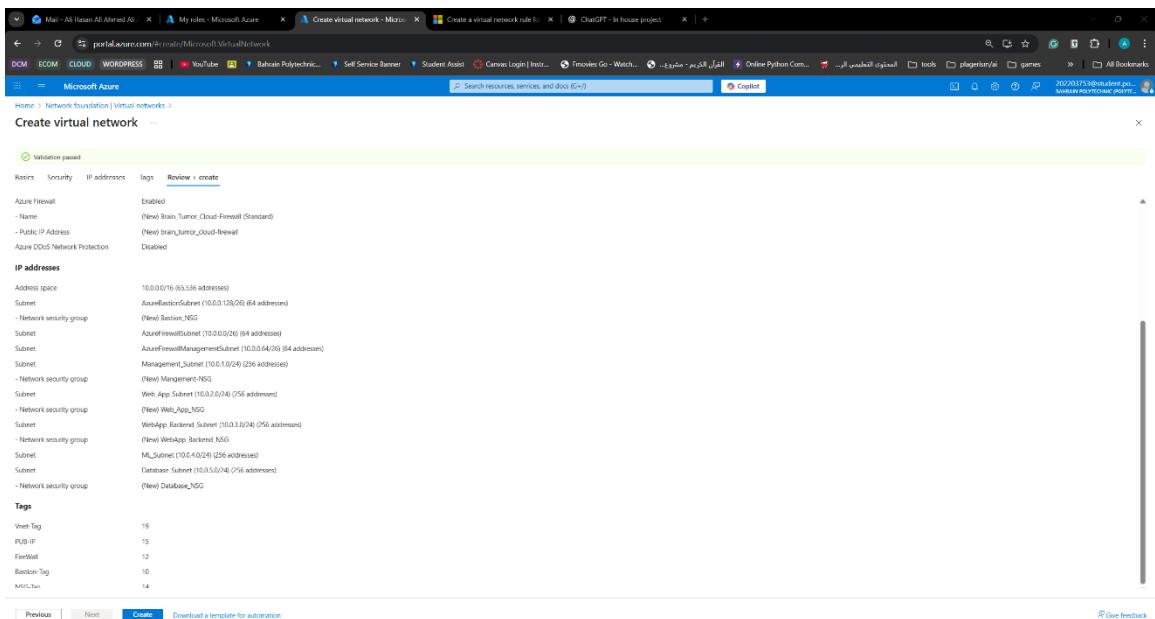


Figure 68: Vnet Creation pt-5

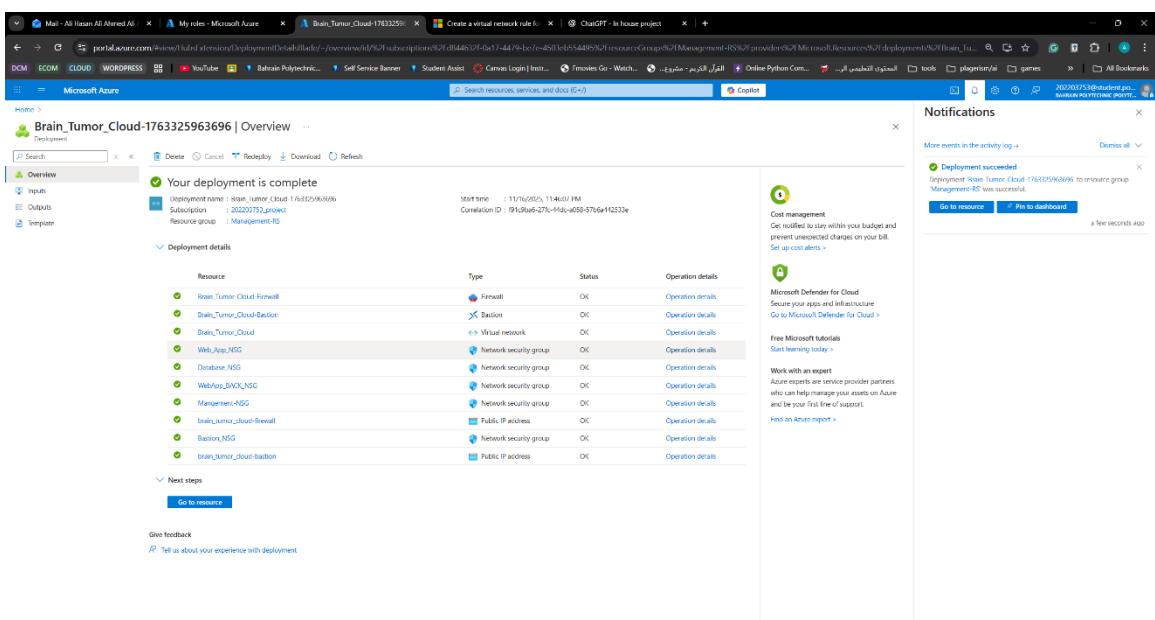


Figure 69: Vnet Creation pt-6

As for the CLI method, Be sure first to install Azure CLI on your device

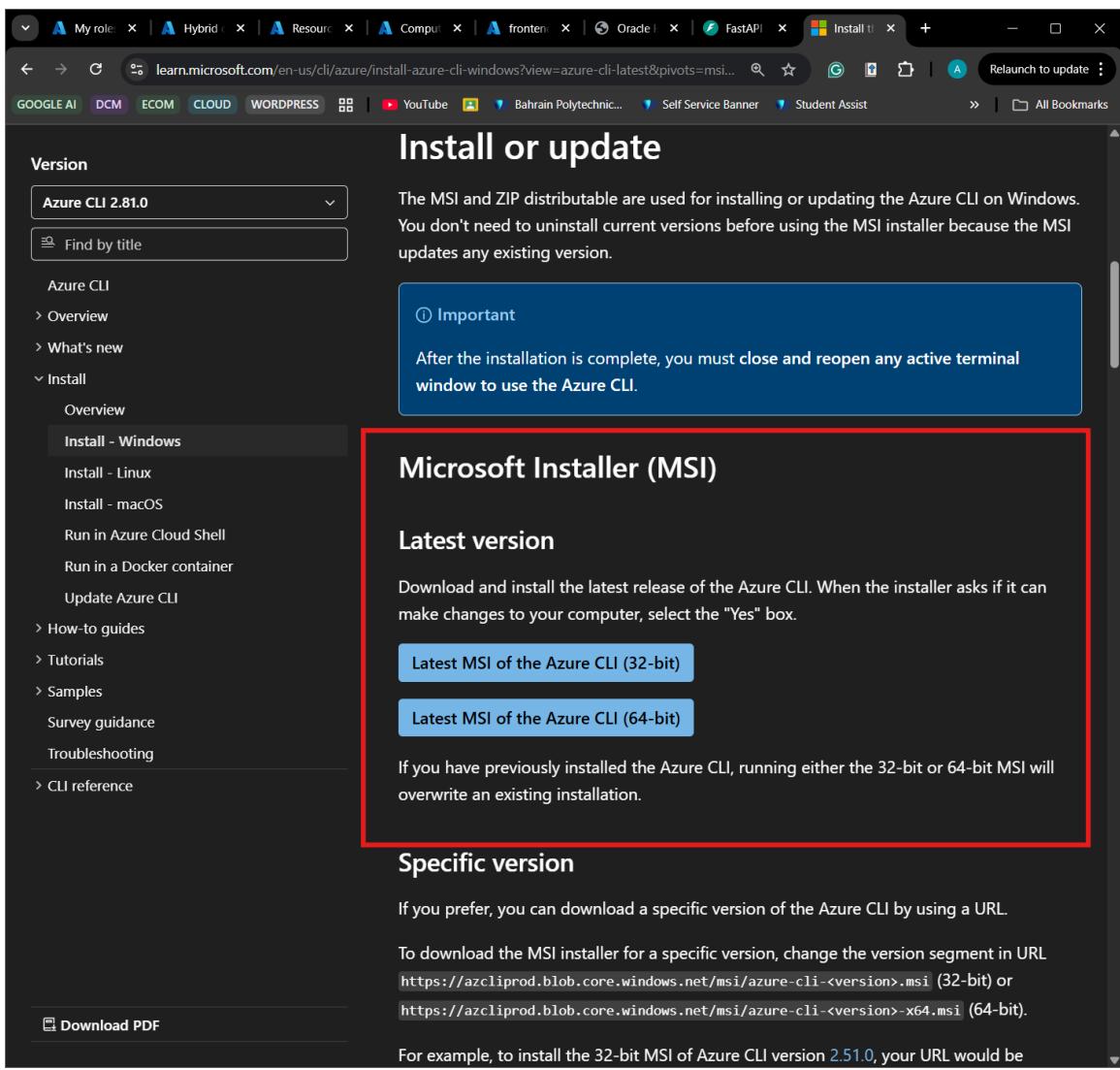


Figure 70: Installation of Azure CLI

To know if you have installed it correctly, use the command “az --version ” as shown below

```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\aliha> az --version
azure-cli          2.81.0
core               2.81.0
telemetry          1.1.0

Extensions:
azure-firewall    2.0.0
ml                 2.40.1

Dependencies:
msal              1.34.0b1
azure-mgmt-resource 23.3.0

Python location 'C:\Program Files\Microsoft SDKs\Azure\CLI2\python.exe'
Config directory 'C:\Users\aliha\.azure'
Extensions directory 'C:\Users\aliha\.azure\cliextensions'

Python (Windows) 3.13.9 (tags/v3.13.9:8183fa5, Oct 14 2025, 14:09:13) [MSC v.1944 64 bit (AMD64)]

Legal docs and information: aka.ms/AzureCliLegal

Your CLI is up-to-date.
PS C:\Users\aliha>

```

Figure 71: Powershell Azure CLI Installation version

Setting up Services

There are Several Services needed, will start with Storage and Database Configurations.

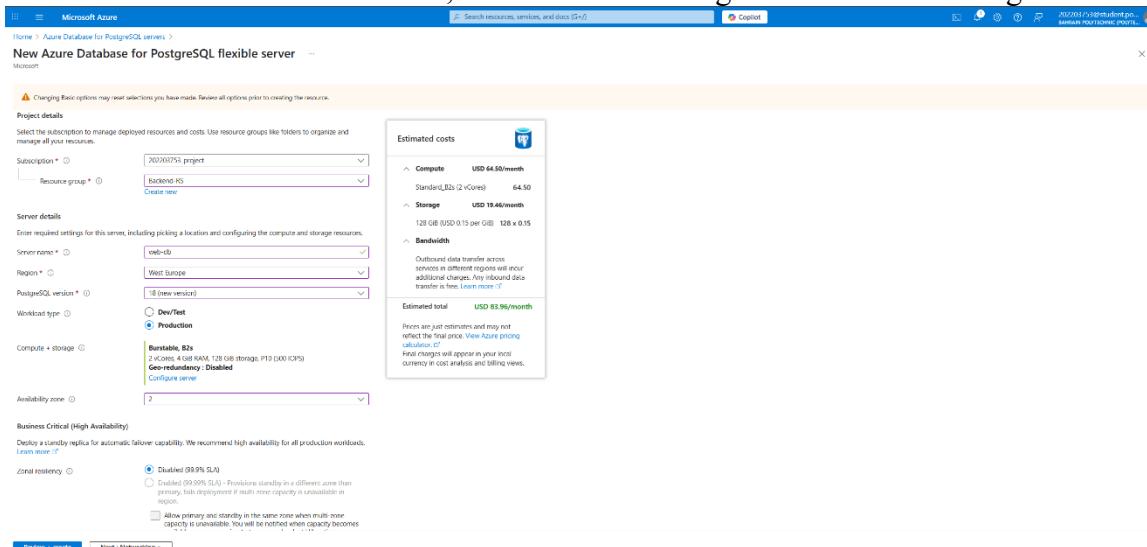


Figure 72: Web-DB configuration

Product details

Azure Database for PostgreSQL
by Microsoft
Terms of use (L7) | Privacy policy (L7)

Basis (Change)

Subscription	202003101_project
Resource group	Backend RS
Server name	web-db
Administrator login	HaAdmin
Location	West Europe
Availability zone	2
High availability	Enabled
High availability mode	Same zone
PostgreSQL version	14
Compute + storage	General Purpose, Dvds_v2 vCore, 8 GiB RAM, 57 GiB storage, F4 (1 vCPU)
Backup retention period (in days)	7 days
Storage auto-grow	Not enabled
Geo-replication	Not enabled
Microsoft Trans. administrators	202003101@studentcloudtechnic.bh
Admin Object/App ID	c03ff9cc-315e-4f70-b139-a952342fb1ad

Networking (Change)

Connectivity method	In-transit access (VNet Integration)
Virtual network subscription	202003101_project
Virtual network resource group	Management RS
Virtual network	Iran_Tunis_Croat
Delegated subnet	Database_Subnet
Private DNS zone subscription	202003101_project
Private DNS zone resource group	Management RS
Private DNS zone	(None) web-db.private.postgres.database.azure.com

Security (Change)

Data encryption	Service-managed key
-----------------	---------------------

Estimated costs

Compute	USD 171.76/month
Storage	USD 4.86/month
High availability	USD 176.64/month
Bandwidth	(Outbound data transfer across persistent different regions will incur additional charges. Any inbound data transfer is free.) Learn more [L7]
Estimated total	USD 353.28/month

Prices are just estimates and may not reflect the final price. View Azure pricing calculator [L7]. Final prices will appear in your local currency in cost analysis and billing views.

Create | < Previous | Download a template for automation

Figure 73: Web DB Configuration Summary

Overview

Your deployment is complete

Deployment name : PostgreSQLFlexibleServer_acf1e4917668416296814cc798a3d411
Subscription : 202003101_project
Resource group : Backend RS

Start time : 11/29/2025, 5:00:16 PM
Correlation ID : 00087605-4ec1-400e-952f-563491e960da

Deployment details

Resource	Type	Status	Operation details
addAdmin-0f06aee2-4d27-4e44-2f03-2c2358de3e53	Deployment	OK	Operation details
web-db	Azure Database for PostgreSQL	OK	Operation details
virtualNetworkLink_20251128T140009213Z	Deployment	OK	Operation details
virtualNetwork_20251129T140009213Z	Deployment	OK	Operation details
privateDnsZone_20251129T140009213Z	Deployment	OK	Operation details

Next steps

Cost management

Get notified to stay within your budget and prevent unexpected charges on your bill. Set up cost alerts >

Microsoft Defender for Cloud

Secure your apps and infrastructure. Go to Microsoft Defender for Cloud >

Free Microsoft tutorials

Start learning today >

Work with an expert

Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support. Read an Azure report >

Figure 74: Summary Deployment

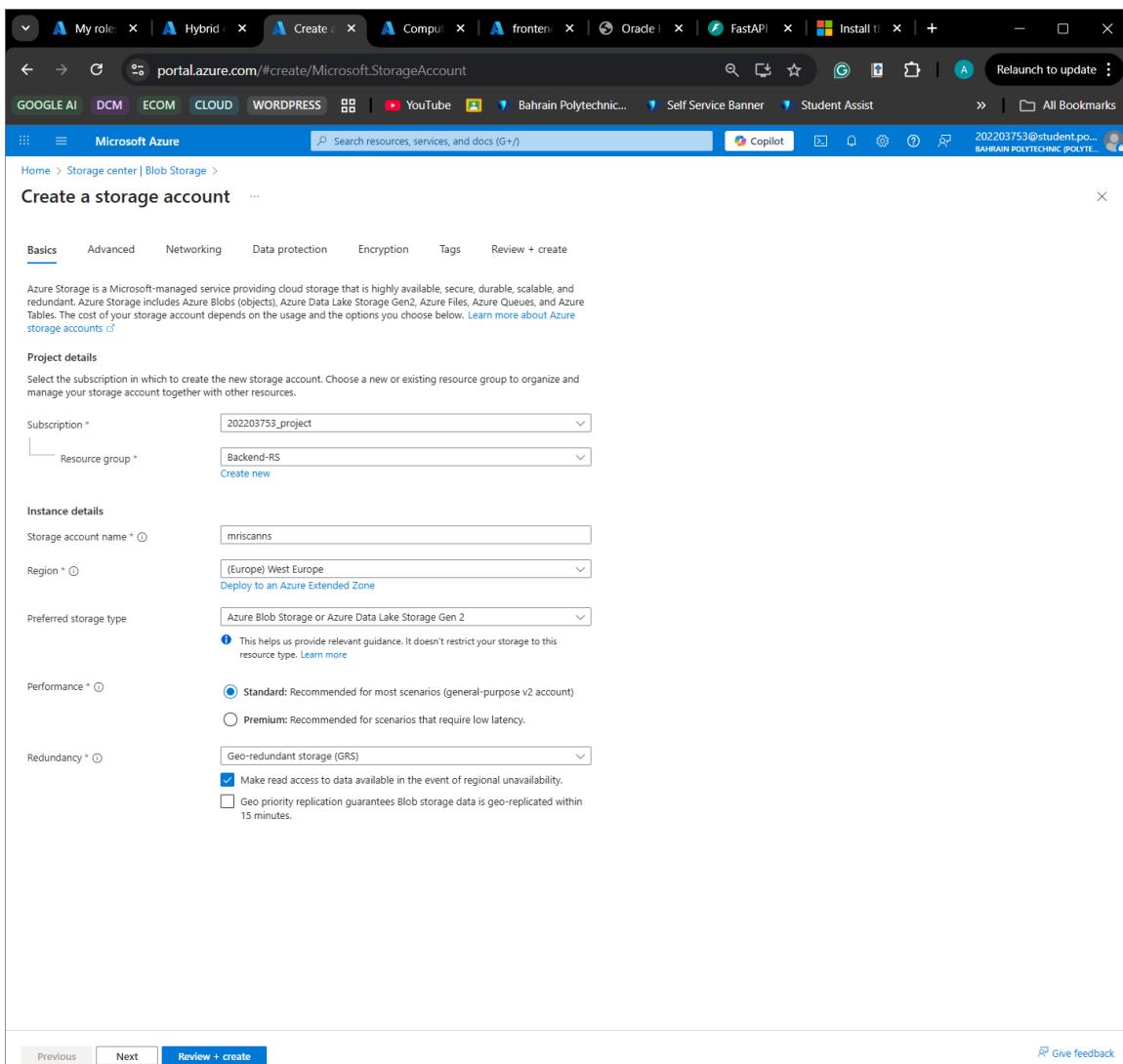


Figure 75: Storage Account creation

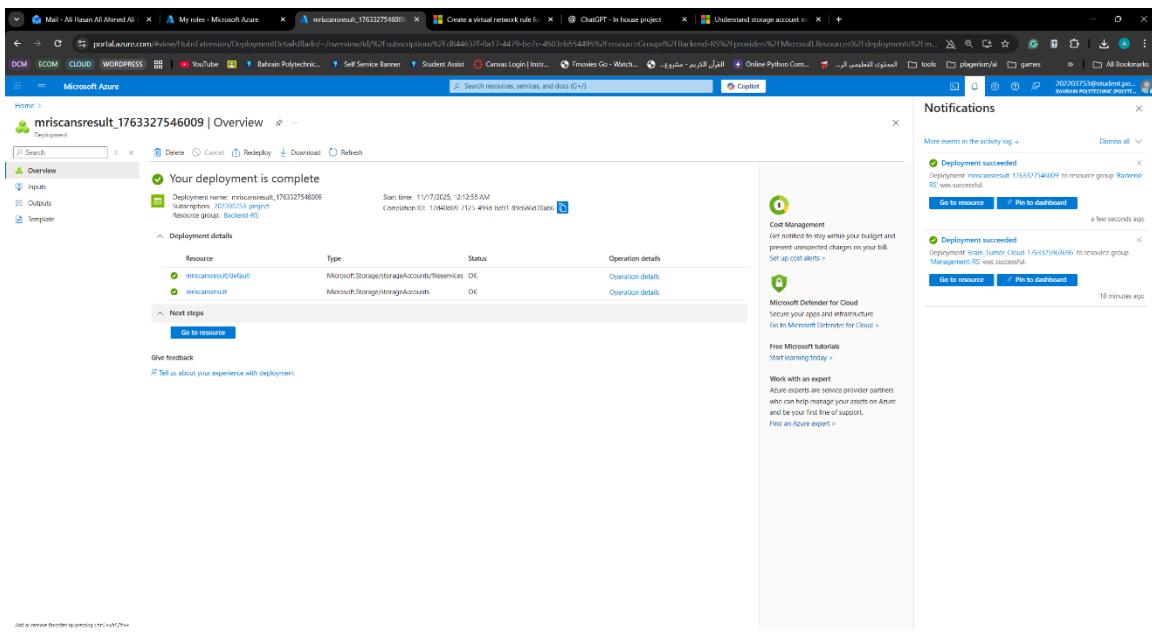


Figure 76: Deploy Storage Account Success

Virtual Machines step-by-step creation were shown in the system Manual to which it will be skipped, though the ARM Template is available on [GitHub](#)

Front-end of the website and Backend logic of the website, Docker was used to containerize the website and ML model.

As for the machine learning model, we first had to create the requirements.txt file with all the libraries we need (Found in GitHub), along with env file and Dockerfile. Below is the commands used to create, build, containerize, and add to Azure containers.

Commands:

```
docker build -t ml-backend:v1 .
```

```
docker run -p 8000:8000 ml-backend:v1
```

```
az acr login --name braintumoracr
```

```
docker tag ml-backend:v1 braintumoracr.azurecr.io/ml-backend:v1
```

```
docker push braintumoracr.azurecr.io/ml-backend:v1
```

```
az containerapp env create `  
--name ml-env `  
--resource-group 202203753_project `  
--location westeurope
```

```
az containerapp create `
```

```
--name ml-backend ` 
--resource-group 202203753_project ` 
--environment ml-env ` 
--image braintumoracr.azurecr.io/ml-backend:v1 ` 
--registry-server braintumoracr.azurecr.io ` 
--ingress external ` 
--target-port 8000 ` 
--cpu 0.5 ` 
--memory 1.0Gi ` 
--min-replicas 1 ` 
--max-replicas 2
```

The screenshot shows three separate Windows PowerShell windows. The first window displays the Docker build command with its logs, showing stages like CACHED, COPY package.json, RUN npm install, and COPY prisma ./prisma. The second window shows the command to tag the image as backendlogic:latest. The third window shows the command to push the tagged image to the Azure Container Registry.

```
--> CACHED [2/7] WORKDIR /app
--> CACHED [3/7] COPY package*.json .
--> CACHED [4/7] RUN npm install
--> CACHED [5/7] COPY prisma ./prisma
--> CACHED [6/7] RUN npx prisma generate
--> CACHED [7/7] COPY . .
--> exporting to image
--> exporting layers
--> exporting manifest sha256:f7560dddf45a5ae75bad78dd9887a11bcd96a7cb9d2269cdb776db6eee8fc9d3a
--> exporting config sha256:94cd79c1bbe3813992d8005ef4f71f179482b2a2e2fbfd039561ecc2cd7eb5b39
--> exporting intermediate manifest sha256:94cd79c1bbe3813992d8005ef4f71f179482b2a2e2fbfd039561ecc2cd7eb5b39
--> exporting manifest list sha256:c79a39fd3a30e16a124eb35c4892c0432a9523f2cf3dde34721e07fe155ae010
--> writing to docker.io/library/backendlogic:latest
--> unpacking to docker.io/library/backendlogic:latest
View build details: docker-desktop://dashboard/build/desktop-linux/desktop-linux/si9jolru0ttqjndg217vifsa
PS C:\Users\ahmed\OneDrive\Desktop\docker stuff\backend\WEBSITE\brain-tumor-backend-main> docker tag backendlogic:latest backendlogicacr.azurecr.io/backendlogic:latest
The push refers to repository [backendlogicacr.azurecr.io/backendlogic]
8c3b0a9e7d86: Pushed
fd1849a5c548: Pushed
ee811238b510: Pushed [====> 24.12MB/247.5MB
e03a8e339d04: Pushed [=====> 22.02MB/25.44MB
8d06ba694611: Pushing [=====> 17.83MB/42.78MB
eaaf4f1e8aa7: Pushed
19cedd69e59a: Pushed
4624ee14dc09: Pushed
19743533ec0d: Pushed
cb3325e64457: Pushed
```

Figure 77: Pushing ML model to Azure

Similar approaches were used for Web backend and frontend. Below is the website deployed on container

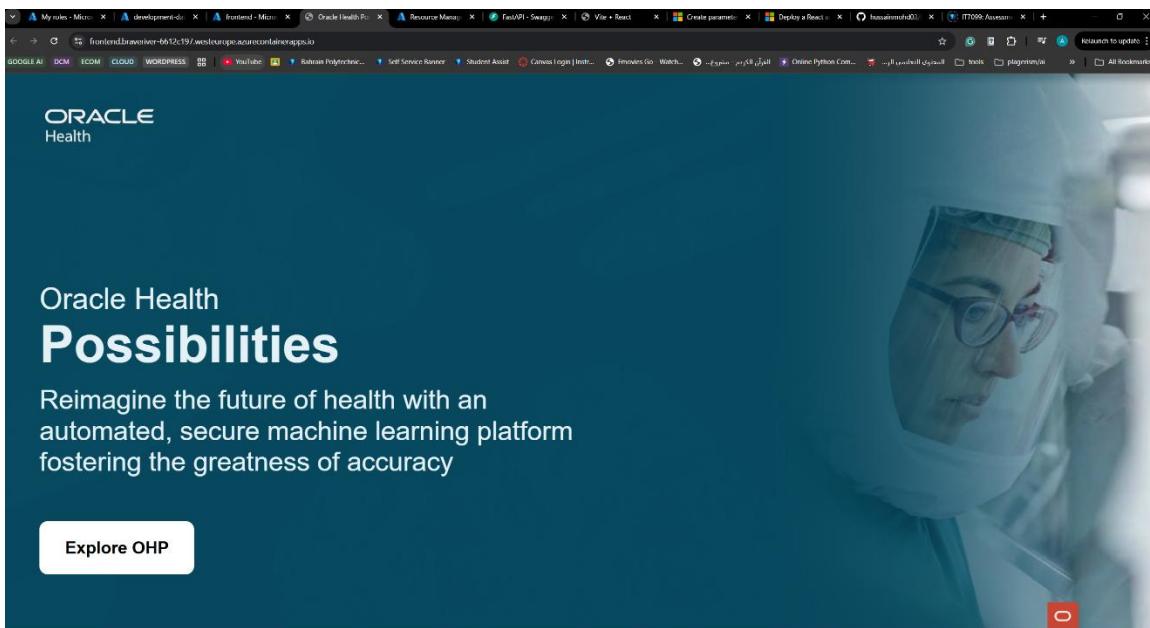


Figure 78: Web deployed

Setting up Security Site-to-Site VPN Configuration

For Site-to-Site VPN creation and configuration, full explanation could be found in Github Repository for the project, below is CLI Commands used to create Site-to-Site VPN

```
az network vnet-gateway create `  
  --name vpngw-cloud `  
  --resource-group Management-RS `  
  --vnet Brain_Tumor_Cloud `  
  --gateway-type Vpn `  
  --vpn-type RouteBased `  
  --sku VpnGw1 `  
  --public-ip-address pip-vpngw-cloud
```

```
az network vnet-gateway create `  
  --name vpngw-onprem `  
  --resource-group Management-RS `  
  --vnet OnPrem-Sim-VNet `  
  --gateway-type Vpn `  
  --vpn-type RouteBased `  
  --sku VpnGw1 `  
  --public-ip-address pip-vpngw-onprem
```

```
az network local-gateway create `  
  --name lng-onprem `  
  --resource-group Management-RS `  
  --gateway-ip-address 172.201.182.91 `  
  --local-address-prefixes 192.168.100.0/24
```

```
az network local-gateway create `  
  --name lng-cloud `  
  --resource-group Management-RS `  
  --gateway-ip-address 172.211.37.101 `  
  --local-address-prefixes 10.0.0.0/16
```

```
az network vpn-connection create `  
  --name conn-cloud-to-onprem `  
  --resource-group Management-RS `  
  --vnet-gateway1 vpngw-cloud `  
  --local-gateway2 lng-onprem `  
  --shared-key S2S-VPN-2025!
```

```
az network vpn-connection show `  
  --name conn-cloud-to-onprem `  
  --resource-group Management-RS `  
  --query connectionStatus
```

Configuration scripts

Most of these scripts are composed of Azure Resource Manager (ARM) templates that declare infrastructure resources declaratively for repetitive deployment tasks with consistency. These templates declare services that are amenable to automation or infrastructure-as-code paradigms, such as storage resources and associated components of the cloud infrastructure.

It is worth mentioning that scripts illustrated here are not all the services that are currently up and running. This is due to certain setups that entail human intervention with regard to the Azure Portal Graphical User Interface, specifically for services for which full automation by means of Azure CLI or Azure ARM templates is limited or not supported at all at the point of deployment. As such, the stages are illustrated conceptually rather than as scripts.

The whole set of configuration files, templates, diagrams, and deployment materials is kept in the GitHub repository of the project and is indeed the central point of all implementation solutions. Only illustrative deployment scripts are included within this document.

Access or sensitive information, like passwords, is consciously not included in the repository on GitHub for the purposes of securing the system. The necessary access details have been clearly documented in this thesis, which has been handled for safe access during the deployment process.

