Executive Summary

The report describes the HeartPath Medical requirements for collecting data as well as storage solutions and analytical processing needs. HeartPath Medical needs systems with strong capabilities to deal with diverse real-time clinical and monitoring data streams. Scalable and secure storage techniques represent must-haves for healthcare organisations to fulfill encryption requirements and achieve operational compliance with data protection regulations. The implementation of complex analytics, especially machine learning becomes essential because these systems produce predictive information about patient treatment and device operation. The infrastructure requirements for cloud deployment demand fast processing of data alongside real-time system monitoring and flexible data source integration. Meeting GDPR requirements together with local data residency standards stands as an essential necessity. The infrastructure establishes HeartPath's foundation to accelerate research partnerships and positions the organisation as a leader in cardiac monitoring healthcare services.

Table of Contents

Introduction

The growing healthcare organisation HeartPath Medical runs multiple clinics throughout many locations. Effective management of distributed clinical and operational data systems represents a fundamental challenge for the organisation. A migration to cloud infrastructure solves their present challenges while providing scalability through expansion (Alghofaili et al. 2021). Clinical integration with operational data creates better treatment results and operational performance improvements. The proposed infrastructure design can establish platforms to enable joint research projects with Universität Tieferwald. The research looks at HeartPath requirements for data needs and reviews potential choices for cloud computing platforms. The research introduces a suggested cloud option as well as portraying a structured architectural framework and proof-of-concept deployment details.

Data Acquisition, Storage and Analysis Needs

Data Acquisition Needs

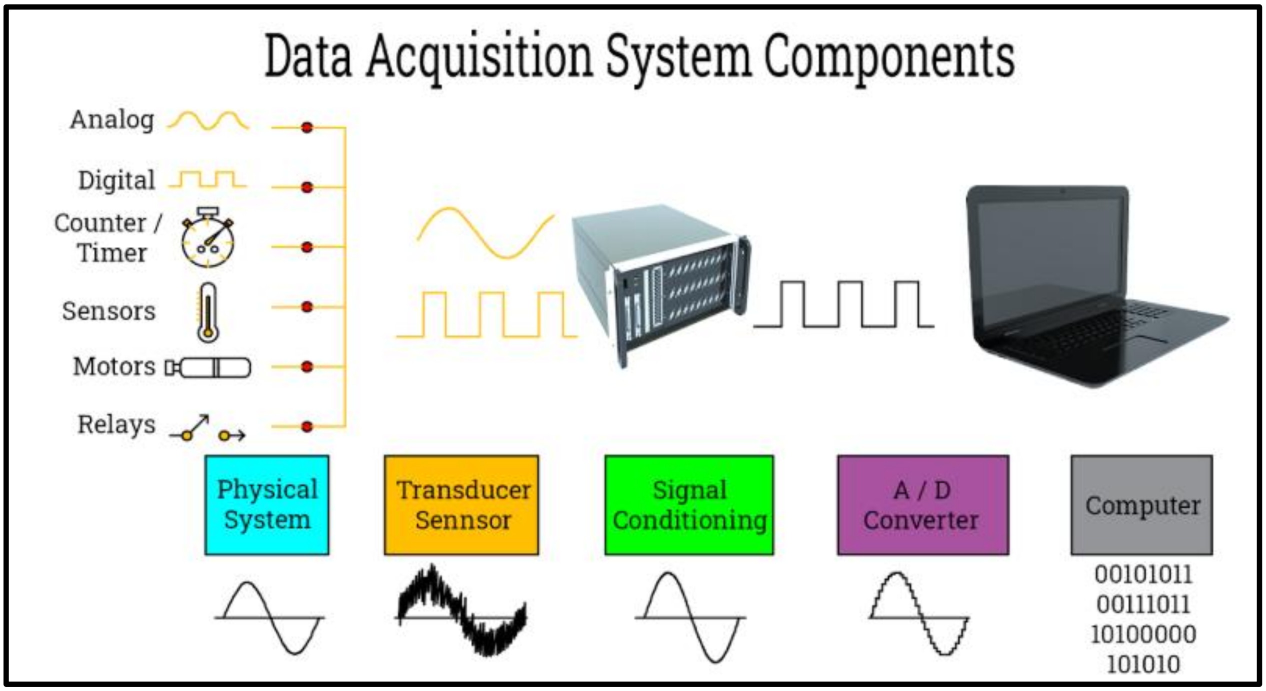


Figure 1: Data Acquisition Components

(Source: iqsdirectory.com)

Requisite medical data originates from the combination of numerous clinics and monitoring devices that operate under HeartPath Medical. The clinical data consists of patient information including diagnostic documentation together with present patient monitoring system outputs

(Tayefi et al. 2021). The operational devices create ongoing health data streams that contain measurements about heart activity combined with device data and battery metrics. The data collection contains heterogeneous information because various devices of uneven age and manufacturing backgrounds produce these data sets. This situation requires strong integration systems for managing this data. Real-time data transmission that supports clinic synchronisation needs to be built into the acquisition system (Santos et al. 2021). HeartPath needs synchronised operational information processing that includes employee database consolidation to produce effective managerial choices.

Data Storage Requirements

Figure 2: Cloud Data Storage

(Source: candourlegal.com)

HeartPath needs a scalable secure data storage environment that supports growing expansion of diverse data types. Weapons protection standards together with data confidentiality needs dictate that clinical information can utilise encrypted data storage operations. The infrastructure requires functionality to manage data formats including those that are structured and semi-structured as well as unstructured. Scalability forms a vital part as HeartPath pursues ongoing acquisitions and expands its monitoring services capabilities (Babiker et al. 2021). The system requires operational integration with clinical data systems to increase overall efficiency. Long-term data accessibility depends on infrastructure storage systems that offer different tiers catering to active and archival data storage categories.

Data Analysis Needs

Large-scale data analysis stands essential for HeartPath because it helps improve both clinical patient results and operational management efficiency. The analysis platform requires predictive capabilities that deliver future-ready insights about device break-downs and patient health conditions. Research staff working with software tools that apply machine learning and enable data visualisation need advanced analytics capabilities to analyse and interpret streaming information from the real-time monitoring system (Razali et al. 2023). The necessity for complex analytic features becomes evident through data evaluation that combines research information with Tiefer Wald scholarship pursuits.

Technical Requirements for Cloud Infrastructure

Real-time monitoring needs a cloud infrastructure that delivers speedy data processing with minimal delay time. Utility requires strong interfacing capabilities that can consolidate information from separate platforms alongside different devices. Legacy systems can connect to modern applications through API compatibility that the infrastructure platform can provide (Colanzi et al. 2021). A important technical necessity of HeartPath requires scalable infrastructure that handles growing data amounts without losing operational capacity. The healthcare platform needs both high availability systems and disaster recovery systems through automated backup solutions and multiple redundant data centers. Operation of the platform depends on integrating advanced analytics features that support big data frameworks.

Regulatory Requirements

Figure 3: Regulatory Compliance

(Source: essentialdata.com)

HeartPath functions in a healthcare environment subject to strict data protection and privacy regulations that can comply with. GDPR regulations in both the UK and the EU decree protected handling practices alongside secured storage requirements for personal data. The system can include other security measures to prevent unauthorised access in addition to the encryption of information during storage and transmission. Data processing in Turkiye along with Switzerland needs to comply with their respective healthcare-specific and data residency legislation. Data processing requests require a transparent auditing system built into the system infrastructure to maintain complete accountability (Soylu et al. 2022). Businesses need to undergo standard compliance audits and prove their certifications by obtaining ISO/IEC 27001 accreditation to fulfill industry requirements.

Evaluation of Cloud Computing Platforms

Cloud computing platforms transformed data processing and management capabilities making that critical infrastructure for HeartPath Medical’s operations. Enterprises can examine crucial characteristics in addition to scalability and cost considerations in the time of analysing major platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). This can also guarantee that regulatory standards are satisfied while protecting sensitive healthcare information.

Amazon Web Services (AWS):

The top cloud computing provider AWS delivers exclusive medical services built for healthcare needs. The platform demonstrates its capability to scale up and run with exceptional reliability. AWS is the number one cloud computing provider that offers exclusive medical services that are developed specifically for healthcare requirements. The platform shows how it can expand and function with high precision. The solution consists of three main services: AWS offers Amazon S3 storage along with Amazon EC2 computing power and AWS Lambda serverless computing. AWS data analytics includes AWS Glue and Amazon Redshift as its primary tools. AWS design includes HIPAA-certified services, advanced cryptographic data protection and strong audit tracking capabilities for security and regulatory compliance (Borra, 2024). The cloud-based architecture of AWS poses a major problem for beginners due to its complex cloud structure and cost structure that demands continuous management to avoid extra costs. AWS Glue and Amazon Redshift are employed by hospital analytics solutions to ensure easy data connection and advanced query capabilities. The use of built-in HIPAA-eligible services, along with encryption and detailed auditing tools, provide security and compliance while protecting data privacy and compliance regulation. AWS's Amazon SageMaker enables healthcare providers to enhance predictive analytics with the help of its machine learning capabilities (Nigenda et al. 2022). This is because new users are likely to struggle with AWS due to its complexity and cost implications that require the need for a professional to manage the costs and utilize the resources to the fullest.**Microsoft Azure:**

Azure delivers robust hybrid cloud capabilities which position the platform well for businesses managing both cloud and on-site infrastructure. Microsoft Azure unifies perfectly with Office 365 productivity solutions and brings together advanced analytics capabilities through Synapse and Machine Learning services implemented on Azure (Klochko et al. 2022). The Azure customers get access to substantial security assets together with privacy standards across “GDPR and HIPAA”. HeartPath focuses on clinics with different IT infrastructures making the hybrid functionality of Azure particularly suitable

Google Cloud Platform (GCP):

“Google Cloud Platform” achieves industry recognition through its innovative data analytics capabilities together with its modern analytical capabilities. The BigQuery service within GCP allows HeartPath to analyze large real-time datasets thereby providing crucial processing capabilities. The GCP platform automatically implements encryption and meets key regulatory standards including “HIPAA” (Callahan et al. 2023). GCP features an ecosystem that trails behind the expansive systems offered by AWS and Azure thus reducing the potential for scalable services and product diversity.

The platform of choice for HeartPath proves to be AWS because it offers high-value healthcare services alongside comprehensive global architecture and robust regulatory compliance programs. HeartPath requires data processing and integration services across its dispersed clinics so AWS provides suitable scalability abilities and advanced analytics solutions. HeartPath finds AWS to offer the optimal combination of features together with compliance standards and reliability for its intricate system requirements.

Cloud Infrastructure Design

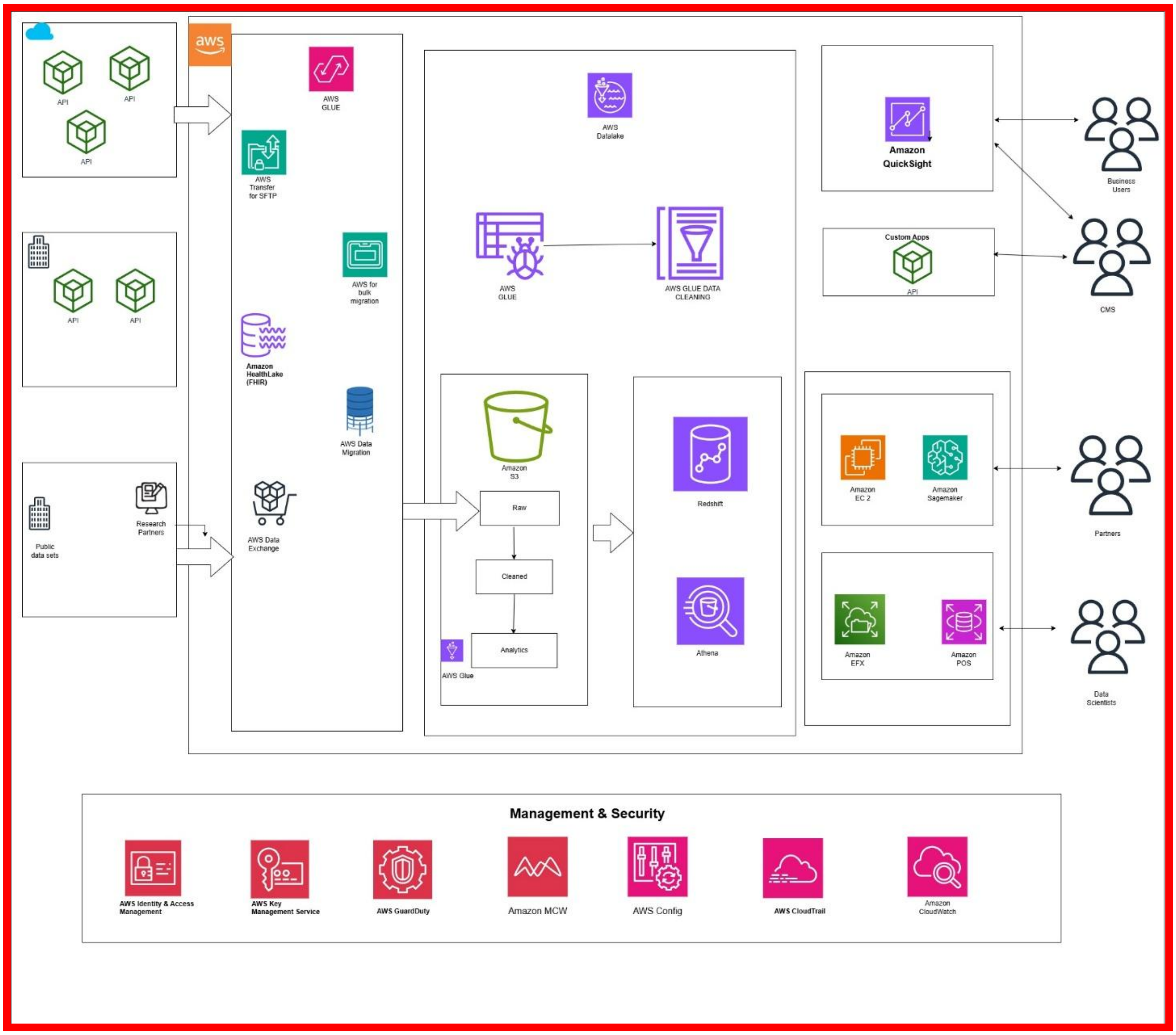


Figure 4: Cloud Architecture

This design uses Amazon Web Services (AWS) as the cloud platform to fulfil the data acquisition, storage and analysis requirements of HeartPath. The solution uses multiple AWS services which deliver scalability and security and adherence to regulations while optimising both processing capacity and analytical capabilities.

Data Acquisition and Ingestion

The data logging solution can utilise **Amazon CloudWatch Events** to detect and launch events triggered by changes in recorded data sources from medical devices and clinical records. Activity monitoring and event recording extends through all systems enabling workflow triggering capabilities. **Amazon SQS (Simple Queue Service)** functionally queues incoming monitoring data and clinical data received from multiple clinics and connected devices (Pu et al. 2024). SQS implements a message queuing system that guarantees real-time data capture while protecting the system from overload conditions.

Data Processing and Integration

AWS Lambda functions serve as platforms for data processing through event-triggered procedures with new monitoring device arrivals. Lambda enables serverless operation that delivers cost-effective scalability together with near real-time data processing. **Amazon SNS (Simple Notification Service)** sends warnings and notifications to different stakeholder groups, such as medical professionals and research team members (Abu-Jassar et al. 2024). These messages are generated by predetermined events, such as equipment faults or important patient status changes.

Data Storage

Patient records along with monitoring device data and research collaboration data can be securely stored in **Amazon S3 (Simple Storage Service).** Service whose object storage solution provides both scalability and durability. Data stored in Amazon S3 Simple Storage Service includes patient records with monitoring device information and research collaboration data. All collected data receives encryption during movement between servers and stays encrypted in the time it is stored as planned to fulfill HIPAA and GDPR healthcare privacy requirements. The data lifecycle management system of S3 can utilise archive strategies to move older information into affordable storage solutions that preserve data longevity and accessibility.

Data Analysis and Research

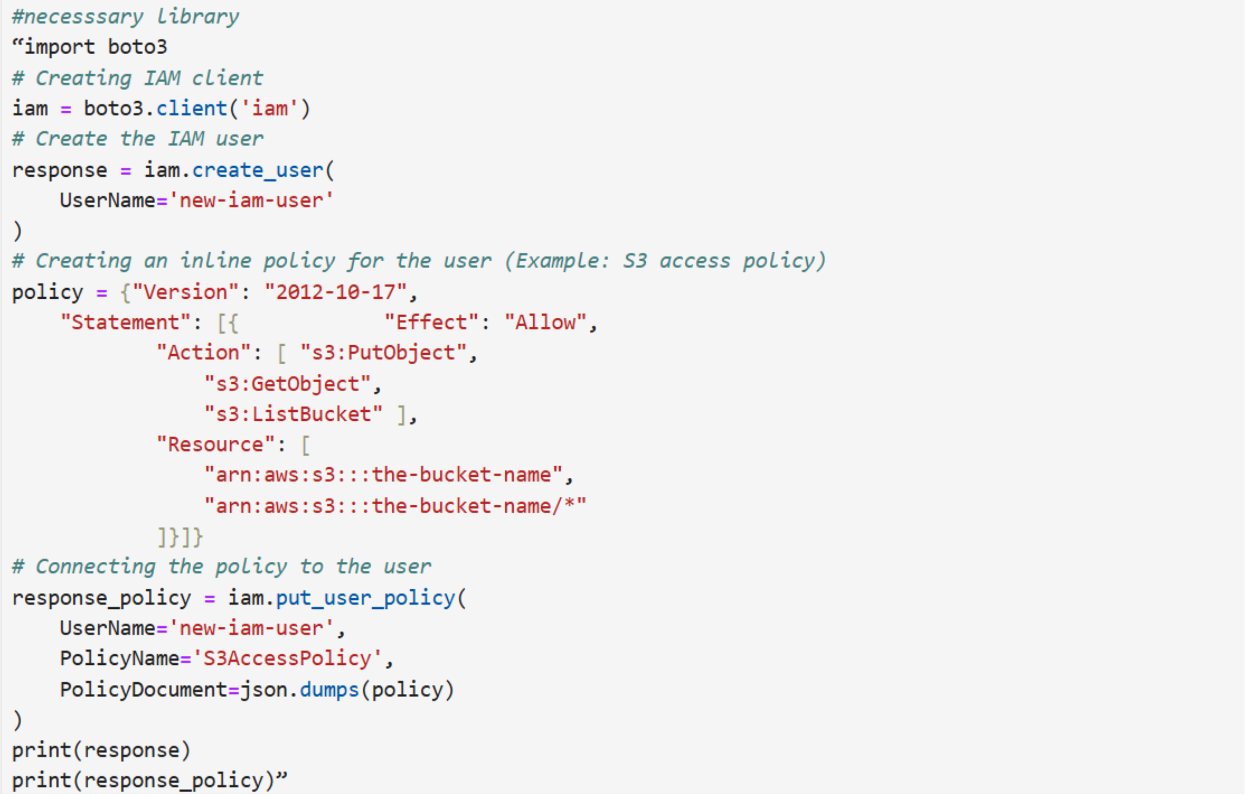
Big data analysis and machine learning operations can use **Amazon DynamoDB** to store structured information that includes patient profiles and monitoring metrics. DynamoDB provides direct access to patient data with low-latency capabilities during both reads and writes through its NoSQL design. **AWS Lambda** handles data processing activities by applying aggregation techniques alongside filtering steps and data transformation before analysis (Mishra et al. 2023). **Amazon SageMaker** researchers can process research data for analysis to enable machine learning models that forecast patient health risks and predict device failures.

Security and Compliance

AWS Identity and Access Management (IAM) manages user permissions to meet regulatory compliance needs. ShiftMagic can enforce IAM-based resource accessibility control to guarantee proper authorisations for managers accessing secure patient data in the cloud platform.

Following are two example Python scripts demonstrating to create an IAM user with a policy and set up a Lambda function to save to an S3 bucket

1. Python script to create an IAM User with Policy

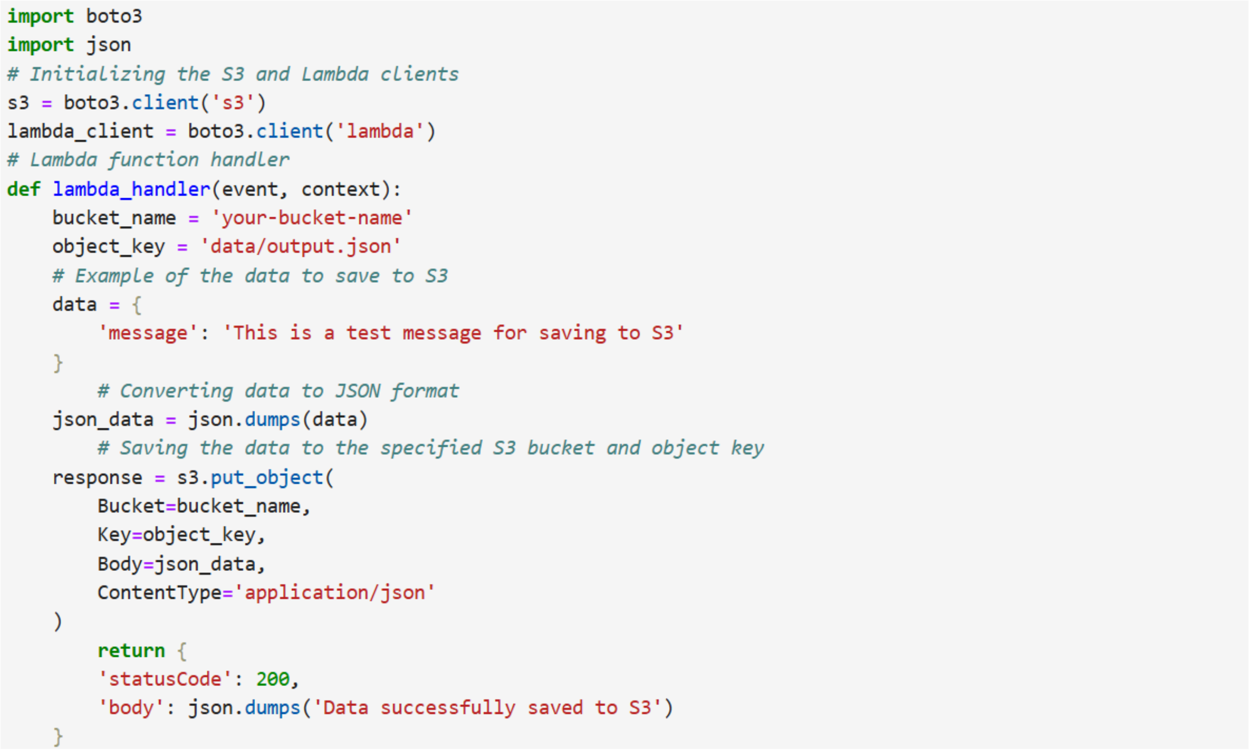


```
#necesssary library
“import boto3
# Creating IAM client
iam = boto3.client('iam')
# Create the IAM user
response = iam.create_user(
    UserName='new-iam-user'
)
# Creating an inline policy for the user (Example: S3 access policy)
policy = {"Version": "2012-10-17",
    "Statement": [{            "Effect": "Allow",
            "Action": [ "s3:PutObject",
                "s3:GetObject",
                "s3:ListBucket" ],
            "Resource": [
                "arn:aws:s3:::the-bucket-name",
                "arn:aws:s3:::the-bucket-name/*"
            ]}]}
# Connecting the policy to the user
response_policy = iam.put_user_policy(
    UserName='new-iam-user',
    PolicyName='S3AccessPolicy',
    PolicyDocument=json.dumps(policy)
)
print(response)
print(response_policy)”
```

Figure 5: Creating an IAM User with Policy

This Python code uses the Boto3 library, which is AWS's SDK for Python to create an IAM (Identity and Access Management) user and then attach an inline policy to that user with specific permissions to Amazon S3 resources. First, boto3.client('iam') creates a client to be able to communicate with AWS IAM services. Then the create_user method is called to create a new IAM user named 'new-iam-user'. After creating the user successfully, an inline policy is defined in JSON format in the structure of AWS IAM policy. This policy provides PutObject (upload files), GetObject (download files), and ListBucket (view bucket contents) permissions to the new user for a certain S3 bucket called 'the-buck- et-name'. These permissions are for both the bucket itself and all its objects ("arn:aws:s3:::the-bucket-name/*"). The put_user_policy method is used to attach this policy to the user, specifying the username as 'new-iam-user' and naming the policy as 'S3AccessPolicy'. Then the responses from both API calls (create_user and put_user_policy) are printed to give details of the newly created user and the policy applied to him/her. Note: There is no import statement for the json library which is required to serialize the policy document.

2. Python script to create Lambda Function to Save Data to S3



```python
import boto3
import json
# Initializing the S3 and Lambda clients
s3 = boto3.client('s3')
lambda_client = boto3.client('lambda')
# Lambda function handler
def lambda_handler(event, context):
    bucket_name = 'your-bucket-name'
    object_key = 'data/output.json'
    # Example of the data to save to S3
    data = {
        'message': 'This is a test message for saving to S3'
    }
        # Converting data to JSON format
    json_data = json.dumps(data)
        # Saving the data to the specified S3 bucket and object key
    response = s3.put_object(
        Bucket=bucket_name,
        Key=object_key,
        Body=json_data,
        ContentType='application/json'
    )
        return {
        'statusCode': 200,
        'body': json.dumps('Data successfully saved to S3')
    }
```

Figure 6: Creating Lambda Function to Save Data to S3

The Python code shows how to create an AWS Lambda function that uses the Boto3 SDK to store JSON data in an S3 bucket. The first lines import the boto3 library to interact with AWS services and the json library to serialize data into JSON format. The S3 and Lambda clients are created via boto3.client('s3') and boto3.client('lambda') but the Lambda client is not utilized within this script. The lambda_handler function serves as the main entry point for AWS Lambda functions which operate in response to events. Within the handler, there is defined both the S3 bucket name ('your-bucket-name') and object key path ('data/output.json'). A test message is placed into a data dictionary and then converted into a JSON string using json.dumps(data). The put_object method from the S3 client uploads this JSON data to the targeted S3 bucket and key and specifies 'application/json' as ContentType to properly handle content. A response with HTTP status code 200 and a JSON serialized confirmation message stating that data has been successfully saved to S3 is returned following a successful upload. Such a Lambda function can be used in event-driven workflows to store data in S3 triggered by API calls, file uploads, and other AWS service events.

HeartPath clinics with other locations can establish **Cross-Account Roles** that provide safe access to their shared systems. **CloudWatch Logs** manages access logs and change records for audit requirements by preserving comprehensive logs that support regulatory adherence and data visibility.

Architecture Diagram

Data monitoring through **CloudWatch Events** activates **Lambda Functions** for processing in the time the architecture performs incoming data detection. The data can move through **SQS Queues** for reliable delivery with alerts delivered through SNS Topics. **S3 Buckets** functions as the secure repository for processed data that DynamoDB and SageMaker use to generate predictive insights alongside **DynamoDB and SageMaker** (Farrow and Jayarathna, 2023). IAM roles together with **Cross-Account Roles** control resource access while commitments to encrypted storage and logging systems verify compliance.

Proof of Concept

The Proof of Concept (PoC) develops and implements the data acquisition processing and storage components of HeartPath Medical's proposed AWS cloud infrastructure. This proof of concept examines the data integration process between various clinical sites and monitoring tools utilizing Amazon Web Services (AWS) platforms. Amazon CloudWatch Events, AWS Lambda, Amazon SQS and Amazon S3 and AWS IAM form the core components of the proposed architectural framework.

The Proof of Concept’s initial stage creates a linkage between medical tracking devices with health clinic IT systems. The system monitors medical data streams to initiate event-based workflows by using Amazon CloudWatch Events. Real-time device data moves through Amazon SQS transportation halls securely as the gadgets are configured for protected and dependable message queuing (Abu-Jassar et al. 2024). The evaluation of the data ingestion system focuses on examining the way it processes a range of device outputs with heterogeneous source inputs.

AWS Lambda operates as the central processing foundation for the system. CloudWatch Events send data to Lambda functions that perform real-time processing while creating necessary data transformations. Determining Lambda function scalability and efficiency requires seeing how the system responds to queries while analysing its data processing capability when information volumes grow. The system sends Amazon SNS notifications that alert users about essential health metric changes through the functionality of this trigger. Amazon S3 provides the storage capacities for data storage operations. Platform as a Service tests secure operations for medical record data including encryption support that confirms adherence to HIPAA and GDPR legal requirements (Zala et al. 2022). Testing of data retention and lifecycle policies confirms that storage schema effectively places older infrequently accessed information into low-cost storage storage tiers. Security tests verify the encryption process for maintaining absolute compliance with current industry encryption and rest and transit security requirements.

The Proof of Concept includes thorough security evaluations alongside compliance testing as a fundamental part. The cloud-based system relies on AWS Identity and Access Management (IAM) to create secure access approaches that define roles together with permissions. The Proof of Concept evaluates security capabilities restricting access to critical information so that authorized personnel maintain exclusive rights to access patient records. Scalability tests are conducted on IAM to validate that access control remains functional in the time of expansion across clinics and in cooperation with Universitat Tieferwald (Ragothaman et al. 2023). The proof of concept evaluation reveals the effectiveness of executing HeartPath Medical's data acquisition, processing alongside data management within the proposed cloud infrastructure environment.

Future Recommendations

Future Implementation

The future implementation of HeartPath requires research into developing advanced machine learning analytics to improve predictions. The analytical models provide improved forecasts about current patient health risks and upcoming device failures. The deployment of AI-driven decision support technologies on expanded infrastructure systems can improve both clinical results and operational performance (Narne et al. 2024). A new security measure blockchain technology ensures trustworthy data records for all important healthcare information.

Scalability and Flexibility

HeartPath can enable its cloud infrastructure to automatically expand that can manage growing data volumes as the organisation grows larger. A scalable infrastructure solution enables the system to scale automatically according to data attractiveness while maintaining costs optimally at high-volume times. There is multiregional structured data placement for future deployments to boost business continuity and disaster recovery capabilities.

Ongoing Maintenance and Security

Maintenance activities need to cover routine system update applications alongside security vulnerability fixes that target newest threats. Implementation HeartPath needs to establish automated systems that can monitor performance and address problems without delay. System compliance checks performed continuously combined with security audits guarantee organizations meet regulatory standards that include GDPR and HIPAA (Lois et al. 2021). Organised training sessions for staff members can result in both infrastructure usability mastery and system security excellence and performance longevity.

Conclusion

HeartPath Medical's cloud infrastructure design satisfies fundamental data retrieval requirements together with data preservation and research needs. AWS stands as the highest platform for scalability while delivering compliance and security benefits. Machine learning integration alongside advanced analytics systems enable improved operational results alongside better patient healthcare outcomes. Future proposals include developing AI-driven analytics and assuring the infrastructure's capacity for development. System maintenance along with security measures represent fundamental elements for both regulatory standards compliance and system performance optimisation. The Proof-of-Concept laboratory testing verified that the proposed solution satisfies HeartPath's current operational needs as well as their projected requirements.

Reference

Abu-Jassar, A.T., Attar, H., Amer, A., Lyashenko, V., Yevsieiev, V. and Solyman, A., (2024). Remote Monitoring System of Patient Status in Social IoT Environments Using Amazon Web Services (AWS) Technologies and Smart Health Care. International Journal of Crowd Science, [Online] 8.

Alghofaili, Y., Albattah, A., Alrajeh, N., Rassam, M.A. and Al-Rimy, B.A.S., (2021). Secure cloud infrastructure: A survey on issues, current solutions, and open challenges. Applied Sciences, [Online] 11(19), p.9005.

Babiker, D.M., Wan, C., Mansoor, B., Usha, Z.R., Yu, R., Habumugisha, J.C., Chen, W., Chen, X. and Li, L., (2021). Superior lithium battery separator with extraordinary electrochemical performance and thermal stability based on hybrid UHMWPE/SiO2 nanocomposites via the scalable biaxial stretching process. Composites Part B: Engineering, [Online] 211, p.108658.

Borra, P., (2024). Comprehensive survey of amazon web services (AWS): techniques, tools, and best practices for cloud solutions. International Research Journal of Advanced Engineering and Science, [Online] 9(3), pp.24-29.

Callahan, A., Ashley, E., Datta, S., Desai, P., Ferris, T.A., Fries, J.A., Halaas, M., Langlotz, C.P., Mackey, S., Posada, J.D. and Pfeffer, M.A., (2023). The Stanford Medicine data science ecosystem for clinical and translational research. JAMIA open, [Online] 6(3), p.ooad054.

Colanzi, T., Amaral, A., Assunção, W., Zavadski, A., Tanno, D., Garcia, A. and Lucena, C., (2021), September. Are we speaking the industry language? The practice and literature of modernizing legacy systems with microservices. In Proceedings of the 15th Brazilian Symposium on Software Components, Architectures, and Reuse [Online] (pp. 61-70).

Farrow, B. and Jayarathna, S., (2023), August. A Serverless Electroencephalogram Data Retrieval and Preprocessing Framework. In 2023 IEEE 24th International Conference on Information Reuse and Integration for Data Science (IRI) [Online] (pp. 221-226). IEEE.

Klochko, O.V., Gurevych, R.S., Nagayev, V.M., Dudorova, L.Y. and Zuziak, T.P., (2022), June. Data mining of the healthcare system based on the machine learning model developed in the Microsoft azure machine learning studio. In Journal of Physics: Conference Series [Online] (Vol. 2288, No. 1, p. 012006). IOP Publishing.

Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A. and Vrontis, D., (2021). Internal auditing and cyber security: audit role and procedural contribution. International Journal of Managerial and Financial Accounting, [Online] 13(1), pp.25-47.

Mishra, S., Alenizi, A. and Dutta, S., (2023). Testing Serverless Applications with AWS Lambda: An Automatic Move to Serverless Architectures. IN THE NAME OF ALLAH, THE MOST GRACIOUS, THE MOST MERCIFUL, [Online] 10(1).

Narne, S., Adedoja, T., Mohan, M. and Ayyalasomayajula, T., (2024). AI-Driven Decision Support Systems in Management: Enhancing Strategic Planning and Execution. International Journal on Recent and Innovation Trends in Computing and Communication, [Online] 12(1), pp.268-276.

Nigenda, D., Karnin, Z., Zafar, M.B., Ramesha, R., Tan, A., Donini, M. and Kenthapadi, K., (2022), August. Amazon sagemaker model monitor: A system for real-time insights into deployed machine learning models. In Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining [Online] (pp. 3671-3681).

Pu, M., Wang, A., Chang, A., Quan, K. and Zhou, Y.W., (2024). Exploring Amazon Simple Queue Service (SQS) for Censorship Circumvention. Free and Open Communications on the Internet.

Ragothaman, K., Wang, Y., Rimal, B. and Lawrence, M., (2023). Access control for IoT: A survey of existing research, dynamic policies and future directions. Sensors, [Online] 23(4), p.1805.

Razali, M.N., Ibrahim, N., Hanapi, R., Zamri, N.M. and Manaf, S.A., (2023). Exploring Employee Working Productivity: Initial Insights from Machine Learning Predictive Analytics and Visualization. Journal of Computing Research and Innovation, [Online] 8(2), pp.235-245.

Santos, M.D., Roman, C., Pimentel, M.A., Vollam, S., Areia, C., Young, L., Watkinson, P. and Tarassenko, L., (2021). A real-time wearable system for monitoring vital signs of COVID-19 patients in a hospital setting. Frontiers in Digital Health, [Online] 3, p.630273.

Soylu, A., Corcho, Ó., Elvesæter, B., Badenes-Olmedo, C., Yedro-Martínez, F., Kovacic, M., Posinkovic, M., Medveščček, M., Makgill, I., Taggart, C. and Simperl, E., (2022). Data quality barriers for transparency in public procurement. Information, [Online] 13(2), p.99.

Tayefi, M., Ngo, P., Chomutare, T., Dalianis, H., Salvi, E., Budrionis, A. and Godtliebsen, F., (2021). Challenges and opportunities beyond structured data in analysis of electronic health records. Wiley Interdisciplinary Reviews: Computational Statistics, [Online] 13(6), p.e1549.

Zala, K., Thakkar, H.K., Jadeja, R., Singh, P., Kotecha, K. and Shukla, M., (2022). PRMS: design and development of patients' E-healthcare records management system for privacy preservation in third party cloud platforms. IEEE Access, [Online] 10, pp.85777-85791.

Appendix

- #necesssary library

```
    “import boto3
    # Creating IAM client
    iam = boto3.client('iam')
    # Create the IAM user
    response = iam.create_user(
        UserName='new-iam-user'
    )
    # Creating an inline policy for the user (Example: S3 access policy)
    policy = {
        "Version": "2012-10-17",
        "Statement": [
            {           "Effect": "Allow",
                "Action": [
                    "s3:PutObject",
                    "s3:GetObject",
                    "s3:ListBucket"
                ],
                "Resource": [
                    "arn:aws:s3:::the-bucket-name",
                    "arn:aws:s3:::the-bucket-name/*"
                ]
            }
        ]
    }
    # Connecting the policy to the user
    response_policy = iam.put_user_policy(
        UserName='new-iam-user',
        PolicyName='S3AccessPolicy',
        PolicyDocument=json.dumps(policy)
    )
    print(response)
print(response_policy)”
```

-
  ```
  import boto3
  import json

  # Initializing the S3 and Lambda clients

  s3 = boto3.client('s3')

  lambda_client = boto3.client('lambda')
  ```

```
# Lambda function handler
def lambda_handler(event, context):
    bucket_name = 'your-bucket-name'
    object_key = 'data/output.json'
    # Example of the data to save to S3
    data = {
        'message': 'This is a test message for saving to S3'
    }
        # Converting data to JSON format
    json_data = json.dumps(data)
        # Saving the data to the specified S3 bucket and object key
    response = s3.put_object(
        Bucket=bucket_name,
        Key=object_key,
        Body=json_data,
        ContentType='application/json'
    )
        return {
        'statusCode': 200,
        'body': json.dumps('Data successfully saved to S3')
```