ARCHITECTURAL DESIGN AND OVERVIEW OF MEDCIRCLE HEALTHCARE APPLICATION

FINAL PROJECT

ENPM665 CLOUD SECURITY FALL 2023

Project members

1. **Name - Garima Sharma**
   Directory ID - garima
2. **Name - Geetika Babu**
   Directory ID - geetika
3. **Name - Samridha Murali**
   Directory ID - samridha

TABLE OF CONTENTS

1. INFRASTRUCTURE CHANGES

The modified healthcare application's infrastructure provides better security, reliability, availability, and robustness. The infrastructure is designed with secure best practices compliant with HIPAA regulations. The modified infrastructure has improved logging, monitoring, threat detection, traffic management, key management, scalability, availability, performance, and security using AWS services.

The architectural diagrams have been constructed separately from the following points of view:

- Architectural Diagram: Patient's view
- Architectural Diagram: Care Provider's view
- Architectural Diagram: IT Support's view

The changes made to the infrastructure are:

- For monitoring added Amazon CloudWatch service to the infrastructure, it provides real-time monitoring and alerting based on application performance and utilization.
- For Vulnerability management added Amazon inspector service to infrastructure.
- For threat detection added Amazon guard duty service to infrastructure for monitoring unauthorized, unexpected, and malicious activities and to generate real-time alerts.
- For securely managing secrets added Amazon Secret Manager service to infrastructure.
- For messaging added Amazon SNS service.
- For logging added Amazon CloudTrail service to infrastructure to increase visibility of actions and to help in incidence response.
- For Traffic management, an Application load balancer has been added to the infrastructure to efficiently distribute traffic to computing instances to increase the availability of applications.
- For High Availability, the Auto Scaling feature has been enabled for computing instances.
- For enhancing application layer security added AWS Web Application Firewall.
- To enhance network layer security added AWS Network Firewall.
- For secure key management added AWS KMS to infrastructure for secure and centralized storage and usage of keys.
- For high-performance, scalable database service added amazon aurora.
- For connecting to the on-prem network and AWS VPC infrastructure we added AWS transit gateway.
- Moved the EC2 instance to a private subnet to reduce the exposure to the internet and increase security. Security groups also
- For high availability, replicas of the infrastructure are maintained in 2 availability zones (us-east-1a and us-east-1b).

- We have enabled warm backup sites as part of disaster recovery to increase the speed of retention of data. To alert data exfiltration from data loss prevention is enabled.
- For segmenting, security groups are created. It reduces the lateral movement of attackers in the network and thereby prevents the spread of attacks in the network.

2. SERVICES AND METHODOLOGIES

The following services and methodologies are crucial for deploying a secure and integrated infrastructure on the cloud. These have been implemented in the updated architectural diagram. These security features introduced in the architectural diagram are worth mentioning. As healthcare industries have very high standards and stricter guidelines for data protection and privacy, the following security features help in meeting these strict regulations and demands and also fulfill compliance requirements e.g. HIPAA regulations.

2.1 AWS KMS Encryption

The S3 bucket, EBS volumes, and RDS are encrypted with AWS Key management service as also visible from the architectural diagram. As specified in the vulnerability assessment report, KMS ensures that the keys are stored, managed, and rotated securely. It encrypts volumes, snapshots as well as data moving between database and web servers. It allows fine-grained access control for the management and usage of the keys [1]. Since care providers have access to confidential patient data inside S3, encrypting the S3 with KMS is a very effective way to reduce any chance of infiltrations by hackers.

Using the AWS KMS Encryption, the following risks specified in the vulnerability report can be mitigated

- RDS was not encrypted. An unencrypted database instance puts both its contents and the underlying storage at great risk of disclosure in the case of a security breach. There is no protection for data in transit or at rest.[1]. Encrypting the DB instance using KMS encryption can mitigate this risk.

- There was also no encryption turned on for the EBS volume. Unencrypted data may not be adequately segregated from other data, which increases the risk of accidental changes, interceptions, or disclosure [1]. Encrypting the EBS volume using KMS encryption can mitigate this risk.

- KMS Encryption was not enabled on the S3 bucket. There is relatively little control over the encryption keys when using SSE-S3 encryption, which is the default encryption for

S3. It might not adhere to all security regulations. Additionally, unlike in the case of KMS encryption, the SSE-S3 keys are not rotated. Because KMS encryption gives us more control over the encryption keys, it's a better solution. Furthermore, it defines certain guidelines that control who has access to the keys and how they can be used [1].

2.2 AWS Secret Manager

The AWS Secret Manager service provides a secure way to store, manage, and retrieve database credentials, API keys, and other secrets. As a healthcare organization like MedCircle can have confidential data stored in databases and other data volumes, the data must be protected at all costs. Developers and other IT service staff may access the database multiple times for various reasons. Thus, it becomes important to have strong passwords as well as a secure place to save and update these credentials. AWS Secrets Manager solves this problem by storing confidential data such as passwords, secret keys, and other private details using dynamic references.

Using the AWS Secret Manager, the following risks specified in the vulnerability report can be mitigated

- The database used by the MedCircle application named ‘MedCircleDB’ had very weak and easily guessable login credentials. Sensitive patient medical information may become accessible to unauthorized individuals as a result, potentially resulting in a data breach. Data loss, data theft, data manipulation, and data integrity problems may result from this [1]. By using AWS Secret Manager, these risks can be mitigated. This service is also integrated with AWS CloudTrail in the architectural diagram for the infrastructure so that logs can be maintained and any unusual activity can be identified.

- Access key ID and secret key were hardcoded in the Output parameter of the .yml file ‘MedCircle-CreateS3Bucket’ and were visible in the Cloud Formation console inside AWS. This is a critical level of vulnerability and can result in severe consequences like a compromise of an AWS account, its services, or more [1]. Because AWS Secrets Manager eliminates the need for hard-coded credentials in application source code, it eliminates this risk completely and as a result, strengthens the overall security of the application. Instead of hard-coding credentials, it allows us to dynamically retrieve credentials as needed by making a runtime call to the Secrets Manager service [2].

2.3 AWS Backup

As healthcare data can include crucial things like patient treatment history, records of allergies to certain medications, previous and latest blood test results, CT scans, etc, there comes a need to have a robust disaster recovery plan in place. This is to ensure that no data is lost in case of a

disaster. As healthcare information makes a big difference in the treatment of a patient as well as help the doctors/nurses to make informed decisions, AWS backup is added to the infrastructure to ensure RDS, EBS volumes, and S3 buckets are backed up properly and can be restored at any time, if required. Backup and recovery policies can be formed and administered using AWS Backup according to the needs of the healthcare organization, for instance, complying with HIPAA regulations. These policies will be automatically applied across different availability zones and regions in AWS.

Using AWS Backup, the following risks specified in the vulnerability report can be mitigated:

- The Medcircle Healthcare System lacked a suitable emergency backup plan. Patients may be put in potentially fatal situations, future treatments may be interfered with, and patients' trust and reputation may be damaged [1]. AWS Backup can eliminate this risk by assuring timely recovery of data and preventing any kind of data loss.

- Extended downtime is one of the major risks found in the MedCircle infrastructure, which is caused by insufficient backup of EBS volumes and RDS. Prolonged delays may result in treatment disruptions and, in severe situations, fatalities. Data transfer, instantaneous retrieval, and modifications are essential. This can be achieved by using the AWS Backup service.

2.4 AWS Network Firewall

AWS Network Firewall is being used in the infrastructure to filter traffic coming from the internet as well as going through the VPC and the subnets. It offers centralized control using AWS Firewall Manager, which can continuously define and enforce security policies throughout the infrastructure. AWS Network firewall is enabled for all availability zones to guard against DDoS and DOS attacks, filter unsecured traffic, and manage the flow of inbound and outgoing traffic [1]. A network firewall is a must to filter out unwanted traffic and maintain the security of the hospital network.

AWS Network Firewall can help mitigate the following risks specified in the vulnerability report:

- Within the health infrastructure, none of the VPCs had a Network Firewall activated. As a result, without any predetermined checks, undesirable traffic can pass through and logging and monitoring become challenging. Data and resources can be tampered with, which could have detrimental effects on the MedCircle healthcare system [1]. Using AWS Network Firewall, malicious or undesirable traffic is filtered out and the security of the network is enhanced.

2.5 AWS SNS

- Amazon Simple Notification Service has been added to the architecture to enable message deliveries and notification alerts in case of hospital emergencies.
- It can accommodate various types of unexpected situations by immediately notifying the hospital staff through this service.
- Alerts can go out to the mail addresses or mobiles of the care providers.
- A scenario where this is useful is in case of unexpected failure or maintenance, Amazon SNS will notify the users that they cannot access the portal for a period of time. Accordingly, the doctors/nurses can plan and manage how to function until the portal maintenance is finished.

2.6 Amazon Aurora

Amazon Aurora is a high-performance, high-availability, fully managed relational database management service offered by Amazon [3]. It has built-in security to provide additional security to the database. It provides continuous backups, Automatic failover, multi-availability zone deployments, and Endpoint failover [3].

Amazon Aurora can help mitigate the following risks specified in the vulnerability report:

- The healthcare application provided is in us-east-a1, in the occurrence of a natural disaster like an earthquake, or flood the entire application and patient data will be lost due to insufficient backup. Amazon Aurora provides continuous backup and can maintain about 15 replicas for multi-region replication [3].

2.7 Amazon GuardDuty

Amazon GuardDuty is an intelligent threat detection service offered by AWS, It continuously monitors and detects malicious activities, breaches, unauthorized access, abnormal activity, and threats in the cloud infrastructure [4]. It analyzes logs from various sources for any malicious behaviors and generates alerts.

Amazon GuardDuty can help mitigate the following risks specified in the vulnerability report:

- Amazon GuardDuty prevents any Missed or undetected security incidents by continuously monitoring the AWS resources and services.
- Amazon GuardDuty provides real-time alerts and prevents Delayed Incidence Response.

2.8 Amazon Site-to-Site VPN

Amazon site-to-site VPN is a service that creates a secure communication tunnel between the on-premises network and Amazon VPC. This is particularly useful for connecting remote offices to AWS infrastructure. Amazon Site-to-Site VPN uses IPsec protocol for establishing secure encrypted connections between sites. IPsec encrypts data to preserve the confidentiality of data in transit. IPsec also preserves the integrity and authenticity of data transmitted.

2.9 AWS CloudTrail

AWS cloud trail provides key features like Logging and Monitoring, Event History, etc [5]. This reduces the risk of delayed incidence resolution. CloudTrail helps the incident response team to quickly investigate the issue and resolve it. This increases the visibility of configurations in cloud resources, making it easier to track unexpected changes in configurations.

2.10 Amazon Route 53

Route 53 is Amazon's Domain Name System service. It is a highly distributed, available, and scalable service [6]. Route 53 is also used to monitor the health of applications. In the infrastructure, AWS Route 53 translated domain names into corresponding IP addresses.

2.11 AWS Application Load Balancer

AWS Application Load Balancer distributes incoming traffic to application instances across availability zones to increase the availability of the application. This can be configured to perform health checks on applications. This service prevents the risk of a single point of failure for the application [7].

2.11 Amazon CloudFront

AWS CloudFront serves as a globally distributed Content Delivery Network (CDN) with edge locations across various regions that deliver web content, media files, and other data, to users efficiently [8].

Amazon CloudFront can help mitigate certain risks specified in the vulnerability report:

- The edge servers cache and store the content to distribute to the closer end-users, thereby optimizing load on original servers, reducing latency, and boosting the overall speed and

performance of the application. This is crucial for healthcare applications where quick access to information is vital.

- CloudFront's distributed computing mechanism contributes to disaster recovery. In case of failure in one location, CloudFront immediately reroutes traffic to an alternate edge location, ensuring continuous service availability and reducing the risk of downtime.

2.12 Amazon CloudWatch

AWS CloudWatch is a comprehensive monitoring and observability service that enables real-time collection, storage, and tracking of various metrics, logs, and events from the application resources. It facilitates the setting up of alarms based on predefined thresholds or metric patterns. When these thresholds are breached, CloudWatch triggers alerts or performs automated actions, aiding proactive issue resolution [9].

Logs and metrics obtained from CloudWatch can be used to detect security anomalies, allowing rapid response to potential security incidents or compliance violations.

Triggers and automated actions facilitate brisk responses to potential security incidents that aid in maintaining high availability and rapid recovery during disaster scenarios.

2.13 Amazon Inspector

Amazon Inspector is an automated security assessment service that helps to identify potential security vulnerabilities, compliance issues, and common misconfigurations within the application resources [10].

Its vulnerability scanning and security assessments align with HIPAA compliance requirements. It helps in identifying and mitigating security issues, and data breaches, ensuring compliance with healthcare regulations.

The inspector examines the severity of identified vulnerabilities and assigns risk scores, enabling prioritization of remediation measures based on criticality, and supporting effective risk management strategies.

2.14 AWS WAF

AWS WAF (Web Application Firewall) is a security service designed to protect web applications from widespread internet threats and attacks. With the help of customized rules and policies, WAF inspects and allows/blocks incoming web traffic. These rules are designed on conditions such as IP addresses, packet headers, query strings, or request attributes [11].

Its functions include filtering and monitoring of HTTP/HTTPS requests aimed at identifying and blocking common web-based attacks like SQL injection, cross-site scripting (XSS), data breaches, and other malicious attacks.

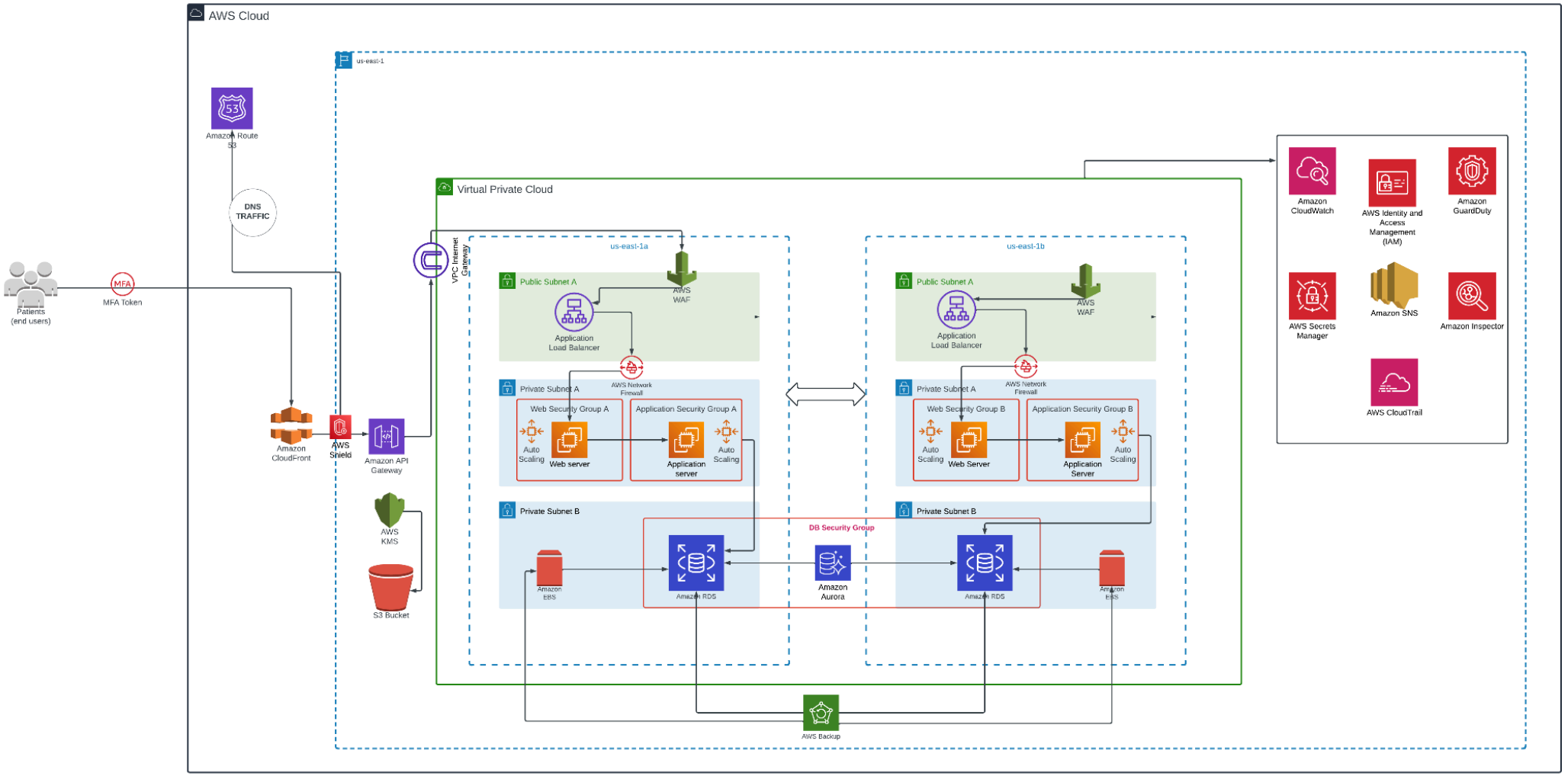
2.15 AWS Shield

AWS Shield provides critical protection against Distributed Denial of Service (DDoS) attacks and fortifies security measures.

It automatically identifies and mitigates DDoS attacks, hence minimizing downtime, and ensuring operability of the critical application resources during potential incidents, failures, and disasters. Continuous monitoring of network traffic helps in mitigating possible threats in real time and enables automatic scaling and adaptability to changing traffic patterns and attack vectors, therefore providing reliable protection without manual intervention.

3. MEDCIRCLE ARCHITECTURE

Following are the architectural diagrams from all three points of view



ARCHITECTURAL DIAGRAM: PATIENT VIEW

3.1 ARCHITECTURAL DETAILS - PATIENT

This segment describes the architecture of the MedCircle infrastructure from a Patient's perspective. The patients utilize their devices to access the healthcare portal for engaging in telemedicine consultations, reviewing their medical test results, managing appointments, and making general inquiries from any location.

The architectural diagram shown above has therefore been put together with careful consideration of these stated daily operations, ensuring security, compliance, and optimal infrastructure performance.

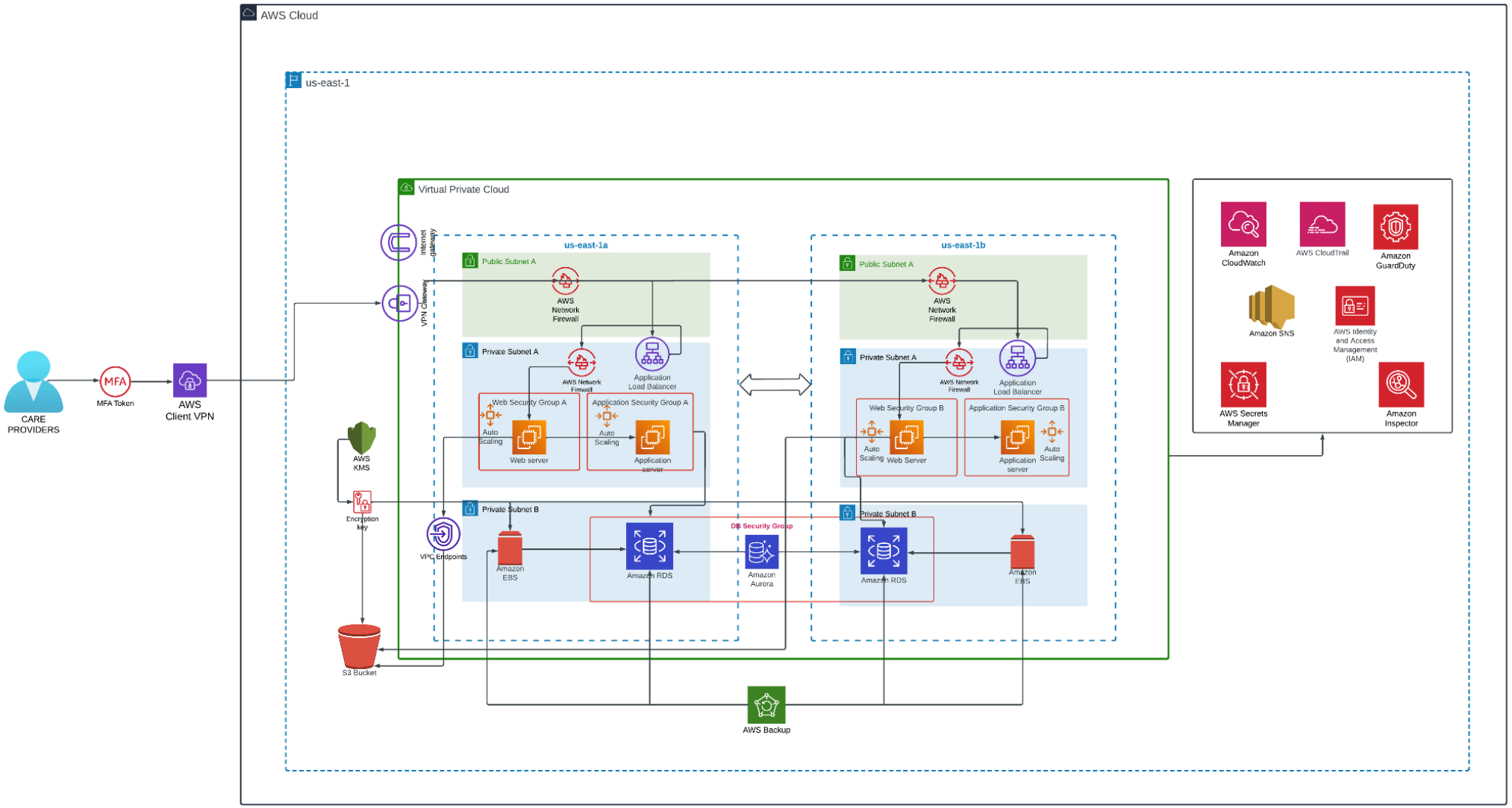
3.1.1 DATA FLOW AND FEATURES

- Patients are registered in the healthcare database system and can therefore log in to the portal to access. They can choose to turn the Multi-Factor Authentication (MFA) on to ensure additional security in the authentication process.
- Users accessing their data and sending requests from various locations connect to an entry-point called *'AWS CloudFront'* which is a Content Delivery Network (CDN) service. CloudFront delivers website content, APIs, and other media efficiently to end users.
- AWS CloudFront is linked to the Amazon API Gateway that manages, secures, and ensures the availability of all the APIs needed to facilitate the healthcare applications' operations.
- The user traffic requests are directed to the appropriate application resources and APIs with the help of a Domain Name System (DNS) service known as AWS Route53. This service is native to AWS and manages domain registration and routing.
- The Gateway is safeguarded by AWS Shield, an AWS service designed to provide enhanced protection against DDoS events, maximizing the availability of applications.
- The requests are forwarded to the resources in Virtual Private Cloud (VPC) via VPC Internet Gateway. The VPC employs Multiple Availability Zones (Multi-AZs) practice, and two AZs (us-east-1a & us-east-1b) in this infrastructure, to ensure fault-tolerance, recovery, and operability during failures, disasters, and incidents.
- The VPC Gateway communicates with the Web Server and forwards the received requests. This traffic goes through the AWS Web Application Firewall (WAF) which is a critical security component for monitoring and filtering the influx of web (HTTP/HTTPS) traffic, and preventing SQL Injection, Cross-Site Scripting (XSS), and other web-based attacks.
- The Application Load Balancer (ALB) in conjunction with WAF intelligently distributes and routes the requests to specific application endpoints. The AWS Network Firewall on

the other hand logs, analyzes, and blocks incoming and outgoing packets based on predefined security rules and policies.

- All three services in conjunction, placed in the public subnet, facilitate Intrusion Detection and Prevention, and secure distribution of internet traffic thereby protecting the internal resources in the private subnets.
- The Web Server and Application Server communicate with each other to serve the user queries. The Web Server processes request-response, delivers web content, and handles the application logic while the Application Server handles core computations in the backend and interacts with Amazon RDS (Relational Database Service) and Amazon Aurora databases for data retrieval and storage.
- Autoscaling is a service used here for supporting scalability and optimization of server's (EC2 instance) capacity based on demand or predefined conditions, ensuring availability as well as cost-efficiency.
- The Amazon RDS is used for database access and management, which in turn utilizes the Amazon Elastic Block Store (EBS) for storage. AWS Backup is an essential service establishing periodic backing up of the data stored in both Amazon EBS and Amazon RDS.

Note: S3 bucket is used for static website hosting and stores application and infrastructure critical data. Hence, patients should not be given access to it as it introduces potential security risks, as it might lead to unauthorized access, data breaches, or unintended modifications to the website content by individuals with access to the bucket.



ARCHITECTURAL DIAGRAM: CARE PROVIDER VIEW

3.2 ARCHITECTURAL DETAILS: CARE PROVIDER VIEW

This section specifies the architecture of the MedCircle infrastructure from the point of view of a Care Provider. Care Providers include doctors, nurses, lab assistants, radiologic technicians, and other hospital staff.

The architectural diagram displayed above has been constructed considering the daily functions of care providers, the security and compliance as well as the high performance of the infrastructure.

3.2.1 DATA FLOW AND FEATURES

- Care providers have a separate portal on the EC2 instance. This hospital portal is specific to be accessed by only the employees of the organization which comprises the doctors, nurses, and the hospital staff. This portal is not accessible by the public and can only be accessed through a private network.

- AWS client VPN refers to a client-based VPN managed by AWS that is used to establish secure connections from any location and restrict access to specific users. It also introduces the feature of connection logging which is a very useful feature from a security point of view. It allows us to log and monitor events to ensure that no malicious user can enter the network [12]. Thus, it is a secure method for employees of an organization to access their portal. The AWS client VPN provides the Care providers with a private link to access the hospital portal and perform their daily functions as can be seen from the architectural diagram.

- The Care providers login to the portal via multi-factor authentication which adds an extra level of security. This multi-factor authentication service is integrated with the application itself. So, there is no need for any external cloud service to provide the same. Multi-factor authentication is highly recommended since care providers can access highly sensitive patient data. Thus, it aims to prevent unauthorized access to sensitive information.

- The traffic flows from the care providers through the AWS client VPN towards the VPN Gateway. This connection is secure and encrypted. From the VPN gateway, this traffic is forwarded to the AWS network firewall to filter the traffic with specified rules and prevent traffic intrusion.

- From the network firewall, the traffic is then forwarded to the Application load balancer. The Application load balancer is used to distribute the traffic among the EC2 instances. This is being used across both availability zones. It helps manage the capacity of the servers according to the traffic load. It increases the efficiency and performance of applications to a large extent. During emergencies, care providers are constantly accessing and modifying the patient details, test results, etc on the application portal to facilitate appropriate treatment. Due to this, there is a high level of traffic and load on the servers. The load balancer manages this type of uneven traffic by uniformly distributing the incoming traffic among the EC2 servers to ensure a smooth experience for the care providers as well as the patients and ensure high availability [13].

- From the application load balancers, the traffic passes through another AWS network firewall. The main objective of this firewall is to filter the traffic between the subnets. It provides an extra level of traffic filtering before it reaches the EC2 instances.

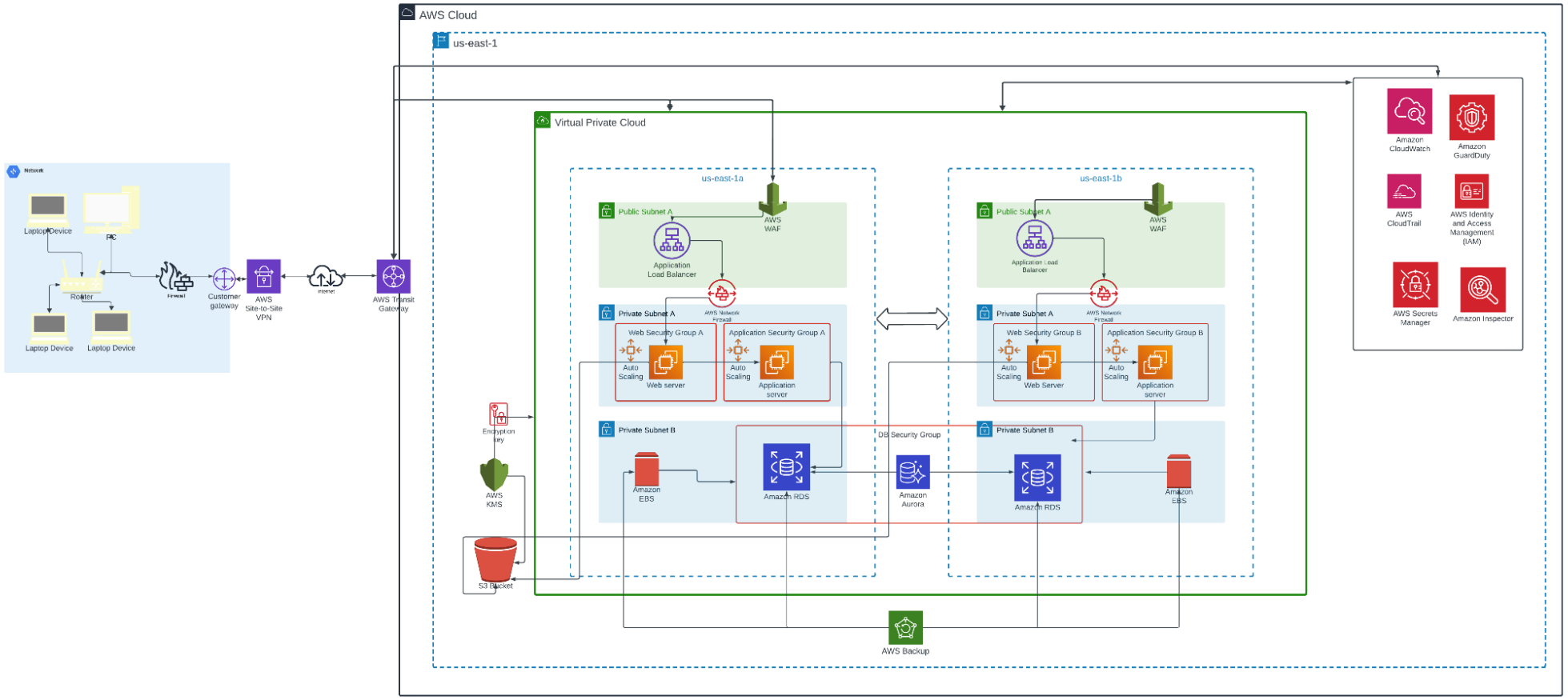
- The EC2 instances are configured with auto-scaling. Auto-scaling helps in managing varied amounts of workloads by scaling the resources accordingly. The instances are scaled automatically based on traffic demand to avoid any excessive costs that may arise when resources are underutilized and to launch additional resources when the existing resources are being overutilized. Hospitals also experience varied traffic loads, which is why the auto-scaling feature is a great way to increase performance and reduce costs in a medical environment [14].

- The Care Providers do not directly access the S3 bucket which contains the patient data and medical results. Instead, different IAM roles are assigned to the EC2 instance to limit the permissions of user access according to their duties in the organization. IAM roles consist of doctor, nurse, lab assistant, and radiologic technician. All the roles have specific read and write permissions for accessing the S3 bucket to view and/or modify patient test results, medication doses, health details, etc.

- As there is no internet connectivity to the private subnets, we have introduced VPC endpoints for accessing the S3 bucket from the Web servers. An EC2 instance that is connected via VPC endpoints does not require a public IP address to communicate and does not leave the AWS global network. This provides a high level of security without compromising availability and bandwidth constraints. This ensures a very safe network for EC2 instances to communicate with the S3 bucket. It also minimizes the attack surface and reduces the chances of exposure to the internet [15].

- RDS and EBS volumes are placed in the private subnet B so that the database and volumes are isolated from the external world. RDS is placed in a DB Security group inside the Virtual Private Cloud to restrict access and specify rules for inbound and outbound traffic to and from the database.

- Public Subnet A is hosting the AWS Network firewall to handle the traffic coming from the internet and from the care providers and redirect it towards the private subnets.



ARCHITECTURAL DIAGRAM: IT SUPPORT VIEW

3.3 ARCHITECTURAL DETAILS: IT SUPPORT VIEW

The IT infrastructure as shown in the architecture diagram contains a premises network and AWS components interconnected through a complex network. In the On-premises network, devices are connected to a router, through a firewall, to the customer gateway. There are multiple roles within the IT team including end-user support, DBAs, security team, system admins, and super admins.

3.3.1 DATA FLOW AND FEATURES:

The data from IT devices on-prem passes through the router and firewall to ensure all security measures are enforced. Data then travels through the customer gateway to establish a site-to-site VPN connection, to securely access the cloud infrastructure. The customer gateway provides information about the on-prem network to AWS. In site-to-site VPN, Data passes through the encrypted link to the AWS infrastructure. This VPN connection has two VPN tunnel tunnels that can be used simultaneously. The traffic through the VPN can be monitored through Cloudwatch as well. [16]. AWS transit gateway is a central hub that connects AWS infrastructure to the on-prem network [17].

The principle of least privilege is enforced in the infrastructure. The access rights of different users are as follows :

- End User support has access to end-user devices for troubleshooting and AWS CloudWatch for monitoring purposes. No direct access to other AWS services.
- Database Administrators have access to Amazon RDS for management, Cloudwatch for monitoring, and AWS backup. No direct access to other AWS services
- Security Team has complete access to on-prem network devices like routers, and firewalls and full access to AWS Guard Duty, Cloudwatch, AWS Inspector, AWS WAF, and network firewall.
- A system administrator has access to Transit gateways, Cloudwatch, AWS secret manager, and AWS backup.
- Super admin has full access to all no-premises devices and full access to all AWS services.

5. REFERENCES

1. Vulnerability Assessment Report: Mid-Term Project (Cloud Security Fall 2023)
2. https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html
3. https://aws.amazon.com/rds/aurora/
4. https://aws.amazon.com/guardduty/
5. https://docs.aws.amazon.com/awscloudtrail/
6. https://aws.amazon.com/route53/
7. https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html#application-load-balancer-components
8. https://aws.amazon.com/cloudfront/?nc=sn&loc=0
9. https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html
10. https://docs.aws.amazon.com/inspector/
11. https://aws.amazon.com/waf/
12. https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/what-is.html
13. https://intellipaat.com/blog/what-is-aws-architecture/
14. https://aws.amazon.com/autoscaling/
15. https://docs.aws.amazon.com/whitepapers/latest/aws-privatelink/what-are-vpc-endpoints.html
16. https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html
17. https://aws.amazon.com/transit-gateway/