ENPM665 – 0101

Final Project

Architectural Design and Overview of Proposed Healthcare Application Platform

Table of Contents

Introduction

The report focuses on the transformation of healthcare applications hosted by Amazon Web Services (AWS), detailing the implementation of a proposed architecture designed to improve performance and security. Understanding the challenges in the healthcare infrastructure and how insufficient services can lead to vulnerability and security breaches. By analyzing the risks in the current architecture, this report aims to provide a comprehensive understanding of AWS service integration and how services can optimize the application against different potential risks. The report underscores the importance of addressing these issues through the implementation of proper service, ensuring robust data security, operationality, and integrity of the overall system.

Current Infrastructure Details

The current infrastructure has various vulnerabilities, which are identifies after theoretical analysis of the infrastructure, and further in the report how these services can be advanced with proper management and can be improved for better performance.

1. Access Control and Key Management:

Maintaining proper authentication for the database is essential to prevent the emergence of a critical vulnerability. Failure to do so could lead to risks such as unauthorized access control, weak credentials in S3, exposure of encryption keys, and potential compromise of system infrastructure or virtual machines. Thus, following the rule of giving the least access needed for authorized jobs. Ensure strong controls are in place for stopping any harm to important data, and regularly checking who has desired permission or access to specific tasks.

2. Web and Application Layers:

A robust network rule management system is required to ensure a safe environment for web and application layers, which specify the types of traffic that are allowed and prohibited. Blindly allowing data from third-party applications into the network, has potential risks to the infrastructure. It is difficult to monitor web requests and the firewall to limit the number of open ports that aren't protected, which will be a security threat.

3. Database Layer:

The use of hard-coded credentials in instances of the database layer poses a significantly higher security risk, potentially exposing the data to an attacker with unauthorized access. This problem is seen as a vulnerability that could lead to the illicit acquisition of valuable resources, through which the confidentiality and integrity of patient data can be endangered. Thus, proper authentication measures are taken to mitigate the threat of unauthorized access control, poor encryption keys, or compromised system infrastructure.

4. Security patching:

Maintaining the overall security of healthcare infrastructure also involves a process of identifying, implementing, and updating security patches. The integrity of cloud healthcare data hinges on the effective configuration of all of these. Neglecting to update the virtual machines will affect compliance and data protection standards. Missing security patches in unpatched virtual environments pose a threat of data breaches and compromising cloud infrastructure.

5. Logging Monitoring:

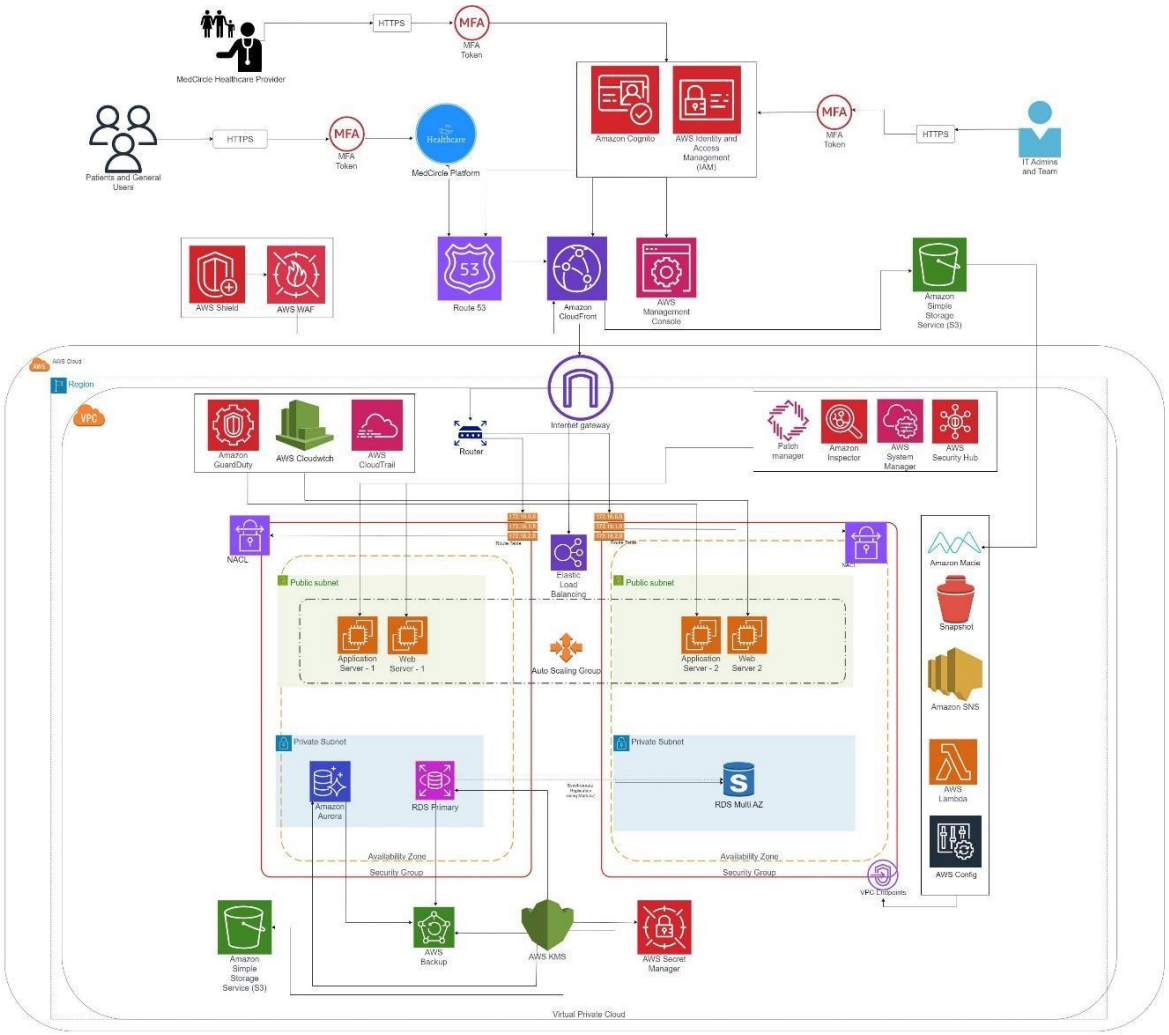
In healthcare applications, sensitive data is involved and handled, inadequate monitoring can result in unauthorized access and manipulation of patients' records, compromising the confidentiality and privacy of individuals. Moreover, inadequate monitoring and logging configuration raise concerns about the system's ability to detect a malicious incident. These issues can potentially result in widespread impacts across the entire infrastructure.

6. Backup and Restore:

Insufficient backup and restore capabilities in AWS healthcare infrastructure can have severe consequences, affecting operability, continuity, and compliance. The instances have no proper protection, leading to the risk of accidental deletion, causing downtime and critical data loss. Additionally, database corruption can expose it to potential data compromise and loss. There is no proper backup plan for any unusual disaster or sudden application crash.

Proposed Healthcare Application Architecture Design

A new proposed architecture design for the Healthcare Application includes all the AWS services to improvise the flow of communication and usage.



Link to design:

https://drive.google.com/file/d/1SOcAj0J9AfjhszcYmsRieATuppqznc2Q/view?usp=sharing

Detailed Overview of Proposed Architecture

The report includes a detailed overview of the services used to improve the overall infrastructure to make it more robust and secure, aligning risk and mitigation in current architecture.

1. Setting up Multi-Factor-Authentication (MFA):

It is a crucial security measure to set up MFA to protect sensitive healthcare data authentication. The additional layer of verification provides secondary protection beyond authentication, increasing access security and reducing the risk of unauthorized account access. This service will enhance security by adding an authentication factor to protect sensitive resources.

Services and Methodologies: *AWS Identity and Access Management (IAM)* and *AWS MFA* offer a flexible approach, allowing the use of different techniques for more secure authentication. Configuring MFA for the relevant accounts and services available for individuals via the AWS Management console or using virtual MFA devices.

2. Enabling S3 bucket object lock:

Object lock ensures the modification setting for an object written to S3, locking it from getting modified or deleted. The main advantage of enabling object lock is safeguarding against accidental deletion of S3 bucket data and providing integrity for data stored by unauthorized modification, enhancing overall regulatory adherence in the AWS S3 environment.

***Services and Methodologies*:** Using services like S3 and IAM, configuring object lock settings in the S3 bucket. Using the *AWS IAM* to manage and access policies to control the permissions for modification of objects.

3. Improving Security Measures Database Credentials:

Considering a good practice to protect database credentials stored with encryption, and access control will reduce the risk of unauthorized access and data breaches. The encryption feature will protect the data, providing operational efficiency and reducing the vulnerability associated with key rotation. The AWS service will integrate with the application, facilitating secure credential storage and secure credential retrieval.

Services and Methodologies: By setting the configuration for *AWS Secret Manager* to securely store and control the database credentials through the features of automatic rotation and encryption. The hardcoded credentials from KMS will be safely stored in the AWS secret manager after configuration.

4. Attach Elastic Load Balancer:

In the AWS architecture, there is a need to implement ELB, to provide high availability, scalability, and efficient distribution of traffic via different Amazon EC2 instances available in different containers. The main reason to use Elastic Load Balancer (ELB) is to make the application accessible and available in heavy traffic load for users.

Services and Methodologies: Configuring the Elastic Load Balancer (ELB) service with integration of Auto-scaling configure it for the available containers and instances, and provides instance reports.

5. Implement proper access control:

Implementing proper control will provide the ability to minimize the potential impact of security incidents by restricting access to unprivileged users. The proper access control will significantly enhance the security posture of AWS resources.

Services and Methodologies: Utilizing the fundamental service of *AWS IAM* for managing access control for roles and permissions available. Defining proper policies and procedures for user roles to perform any actions on resources. Creating proper groups and granting the least privileges according to the user role.

6. Encrypt Data for RDS:

Confidentiality of patient data is always a top priority and leaving the data unsecured pose a threat of data breach through unauthorized access and violation of HIPAA privacy regulations. Encrypting the data at rest or in transit for RDS is crucial. RDS encryption protects against unauthorized access.

Services and Methodologies: *AWS RDS* Encryption is a service that provides ciphering for the data present in RDS instances and through *AWS KMS*, the encryption keys can be managed easily in the architecture.

7. Permitting VPC Flow Logs:

Enabling VPC flow logs is a proactive measure as their absence would result in missing essential updates for security monitoring, compliance adherence, and visibility even during troubleshooting. Critical insights are missed if it is disabled, compromising the network and security issues flow logs allow better network visibility as they contain inbound and outbound traffic.

Services and Methodologies: Configuring VPC as a service provides best practices for reviewing and monitoring the data logs. Configuring the VPC flow logs in the architecture allows log monitoring for the S3 bucket.

8. DNS Firewall configuration:

To address the security concerns related to DNS and DDoS vulnerabilities, the DNS Firewall configurations are crucial. DNS spoofing, cache poisoning and DDoS attacks might occur if it is not implemented. Following the firewall rules precisely filters and blocks malicious domains, preventing unauthorized access and securing the data of patients for hospitals. Route 53 is scalable, efficient, and reliable to work across different regions. It easily acquires connections with other AWS services.

Services and Methodologies: Integrating *Amazon Route 53* provides resolver rules, allowing the creation of firewall-like rules for DNS queries in RDS. Analyzing and filtering DNS logs leverages threat intelligence and enhances the security posture.

9. Deploy traffic flow via HTTPS:

Deploying traffic flow via HTTPS, ensues the data flow is encrypted during transmission. It allows servers to authenticate servers following standard facilitated with by different risks of tampering with data and preventing attacks. The deployment will improve security compliance and is an essential part of successful transmission.

Services and Methodologies: Configuring a web server with HTTPS, along with AWS IAM managing user roles through configuration and integrating traffic flow for secure network configuration.

10. Improve Patch Management:

Patching is a critical aspect of maintaining stability and functionality. A proper patching mechanism is required in an AWS infrastructure to timely protect the system, data, and network from different unwanted and unknown cyber threats. It should be prioritized for the overall security of the system. It should be regularly implemented as a good security practice.

Services and Methodologies: Conducting a regular vulnerability assessment using AWS services to track changes, configuring Patch Manager with other services creating rules for patching and tagging instances to groups.

11. Implement Web Application Firewall (WAF):

To overcome the threat of web-based attacks such as SQL injection, cross-site scripting, and other application layer vulnerabilities, a web access firewall is integrated. WAF mitigates these risks by acting as a proactive barrier between web applications and the internet where it also filters the HTTP traffic for potential cyber-attacks. Web Application Firewall can defend against OWASP (Open Web Application Security) and injection attacks. It also provides real-time monitoring & logging with compliance support.

***Services and Methodologies**:* Configuring *Amazon WAF* with managed ruleset that includes a regular update on potential threats. Custom rules can be defined and tailored based on the security requirements. Configuring WAF around the application load balancer enhances scalability.

12. Configuring rules for NACL:

Network access control lists act as a security layer, controlling all the inbound and outbound traffic at the subnet level. Improper configuration of NACL leads to data breaches and compromised overall security. Network segmentation and isolation is the best practice followed in NACL as it restricts lateral movement within the healthcare infrastructure. The least privilege principle protects against unauthorized access and data breaches.

***Services and Methodologies**:* Services like AWS Security Groups operate at the instance level, managing the network traffic like NACL at the subnet level. Secondly, Amazon VPC will help in setting up a customized architecture for users' needs.

13. Integrate Auto Scaling

Auto-scaling handles various workloads efficiently to ensure optimal performance and proper utilization of resources. It allows the infrastructure to auto-adjust its capacity based on demand for user traffic and ensure the effective allocation of appropriate resources. Certainly, the flexibility and scalability of workload and resources create an overall impact on the performance of individual users.

***Services and Methodologies**:* Integration of Auto-scaling distributes the overall traffic across multiple targets like EC2 instances in the architecture. When applied in conjunction with ELB, it ensures an even load distribution and has fault tolerance.

14. Implement Real-Time Monitoring

In AWS, auto-scaling is a common practice to dynamically adjust resources based on demand. Real-time monitoring is necessary to get insights into resource utilization, enhancing the overall operational efficiency, security, and performance of your AWS environment.

Services and Methodologies: *AWS CloudTrail* and *AWS CloudWatch* together can help in implementing real-time monitoring in AWS effectively. CloudTrail provides a detailed record of API calls made on AWS accounts, while CloudWatch allows to collection and analysis of logs and metrics.

15. Enable AWS Inspector

Requirement: It helps you identify vulnerabilities and security issues in your applications and infrastructure. Other than that, there are regulatory compliance requirements that mandate regular security assessments. AWS Inspector performs automated security assessments to detect vulnerabilities and weaknesses in your AWS resources. It helps to address potential security risks promptly, reducing the likelihood of security breaches and data exposure.

Services and Methodologies: The assessment targets represent the AWS resources that want to assess for security vulnerabilities. This could include EC2 instances, Amazon RDS databases, and other relevant services.

16. Creation of Snapshot:

Elastic Block Store snapshots are an important component of recovery strategies since they serve as backups for data stored on EBS volumes. However, with proper key management and encryption, this data is safe from illegal access, raising the possibility of sensitive information being revealed. The security requirements for data at rest are not being met in this case.

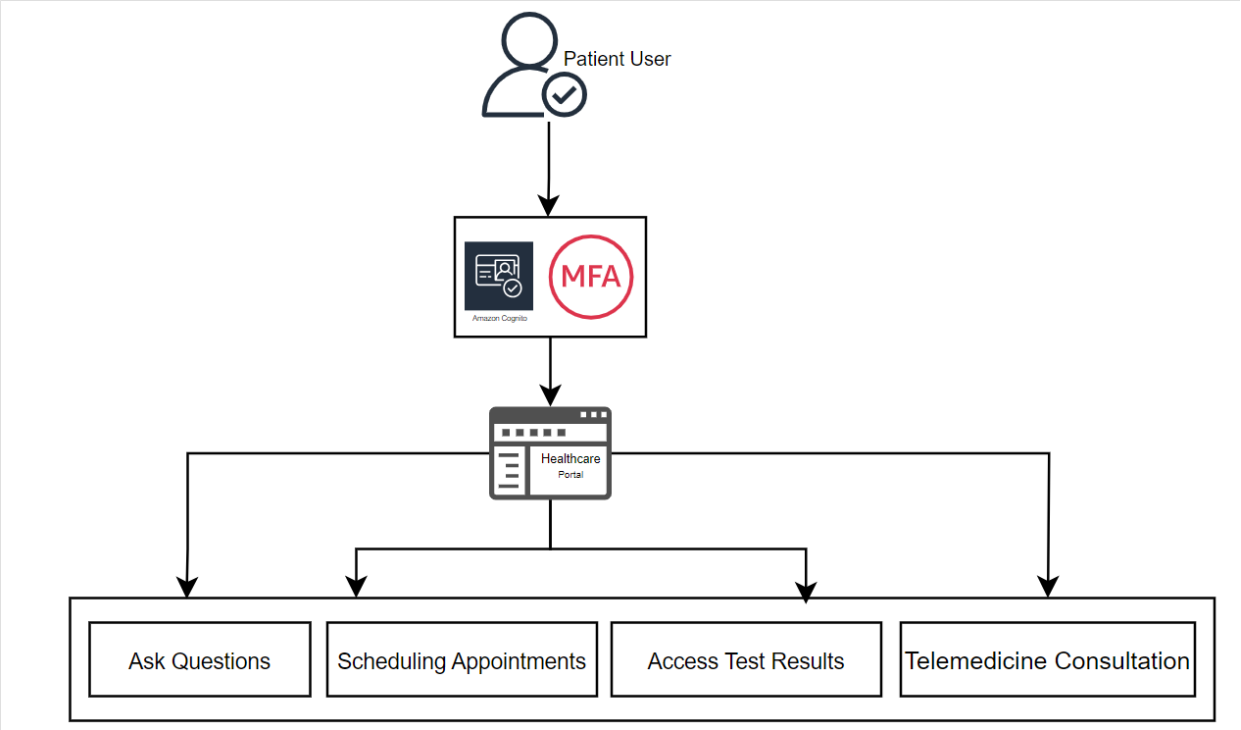
Services and Methodologies: By implementing a secure methodology for regular snapshot schedules, ensuring timely backups. Encrypting protocols can then be applied to safeguard snapshots and mitigate unauthorized access.

17. Design Backup Plan:

Designing a backup plan in Amazon Web Services (AWS) is essential for several reasons, all of which contribute to ensuring the availability, durability, and resilience of your data and applications. This simplifies the backup process by allowing you to create, manage, and monitor backup plans in a single console.

***Services and Methodologies*:** *AWS Backup* is a fully managed backup service that makes it easy to centralize and automate the backup of data across AWS services. Setting up Multi-AZ for RDS instances will help in mitigating the potential threat, supporting replication of databases across multiple zones and provides failover support in case of zone failure.

Architecture details from the Patient's Point of View:



Img 1.1 Architecture flow from Patient's Point of View.

Usage of non-trusted devices to access the application portal:

Patients accessing the portal must prioritize security by using trusted devices, secure connections, and avoiding public computers. In the AWS framework, providers enter through a web application instance using authorized credentials and Multi-Factor Authentication (MFA). The portal integrates with Amazon Cognito and Identity and Access Management (IAM), ensuring a secure sign-up and sign-in experience. IAM roles and policies control access, permitting only authorized entities to execute tasks aligned with their assigned privileges.

Accessing Reports:

Patients efficiently retrieve test results via the application's interface, ensuring swift access to crucial health information. AWS employs the Relational Database Service (RDS), ideal for applications reliant on a relational database model and SQL queries. This facilitates seamless data retrieval, particularly in scenarios critical for business applications, e-commerce platforms, and content management systems.

Scheduling Appointments:

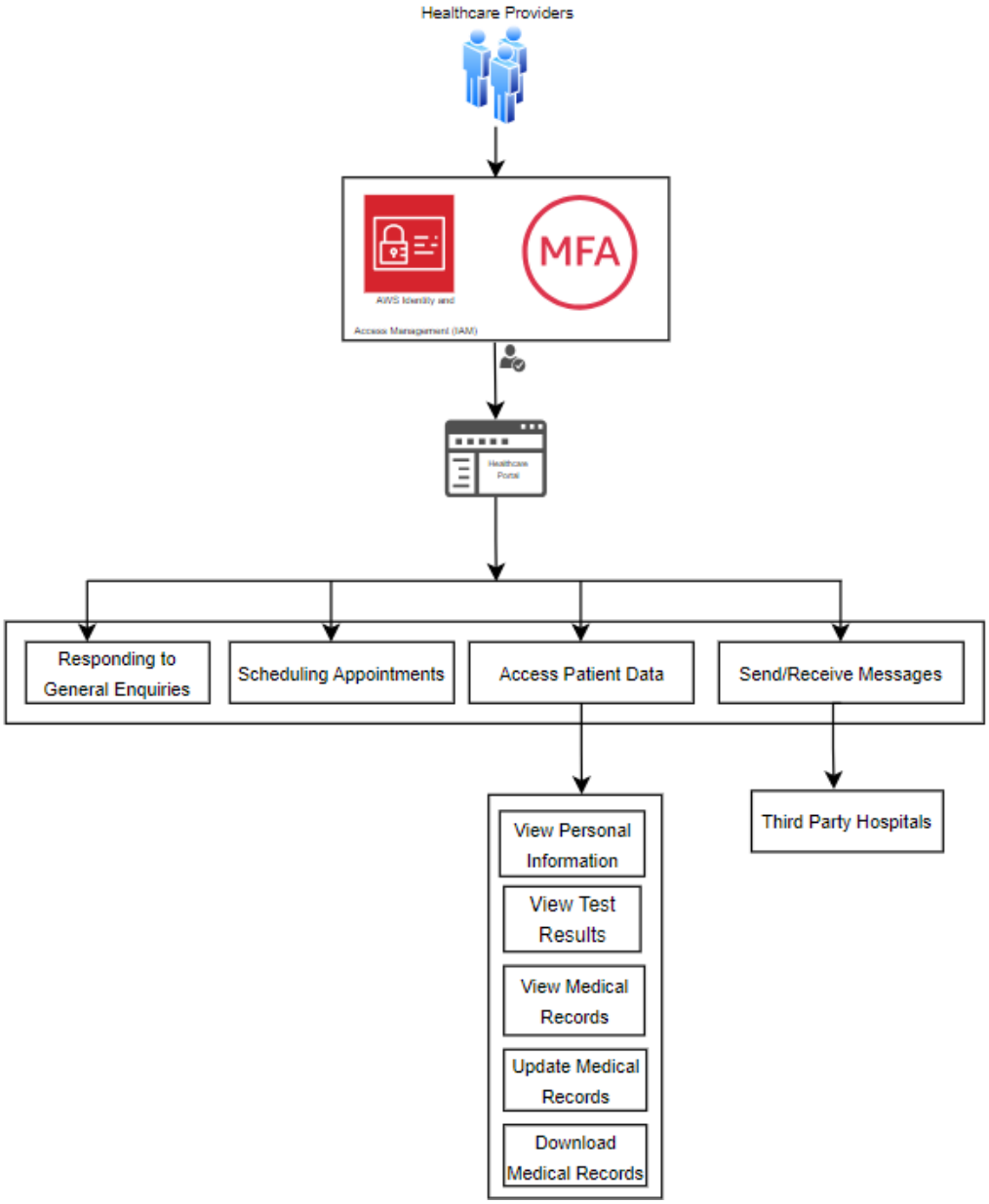
Patients can effortlessly schedule appointments within the app, enhancing the efficiency of healthcare services. The application's scheduling feature aims to support healthcare providers in

effective resource management, ultimately reducing appointment wait times. Utilizing AWS Lambda, the app employs serverless functions to respond to API calls, ensuring the seamless handling of tasks such as appointment scheduling, availability checks, and notifications. This integration enhances the overall healthcare experience for users.

General Inquiries and Interaction:

Patients actively use the application for general inquiries and symptom recognition, contributing valuable information about their health. This collaboration enables healthcare professionals to offer personalized guidance more effectively, enhancing the overall efficiency of healthcare delivery. The application seamlessly integrates with AWS S3, leveraging its scalable and secure storage capabilities to house informational resources such as FAQs, brochures, and educational materials. This ensures accessible and organized information, further supporting patients in their healthcare journey. Additionally, patients utilize the SNS (Simple Notification Service) within the application for secure communication, enhancing the effectiveness of interactive and informational exchanges between patients and healthcare providers.

Architecture details from the Care Provider's Point of View:



Img 1.2 Architecture flow from Care Provider's Point of View.

Access and Authorization:

The providers will access the system through a portal hosted on a web application instance using authorized credentials via MFA login. The portal provides an overview of the application services, and the Amazon Cognito and IAM services provide the required access and authentication to get the required permission set for performing tasks according to privileges assigned to roles signed in. Access control with IAM roles and their policies will make sure only authorized entities have the necessary permission.

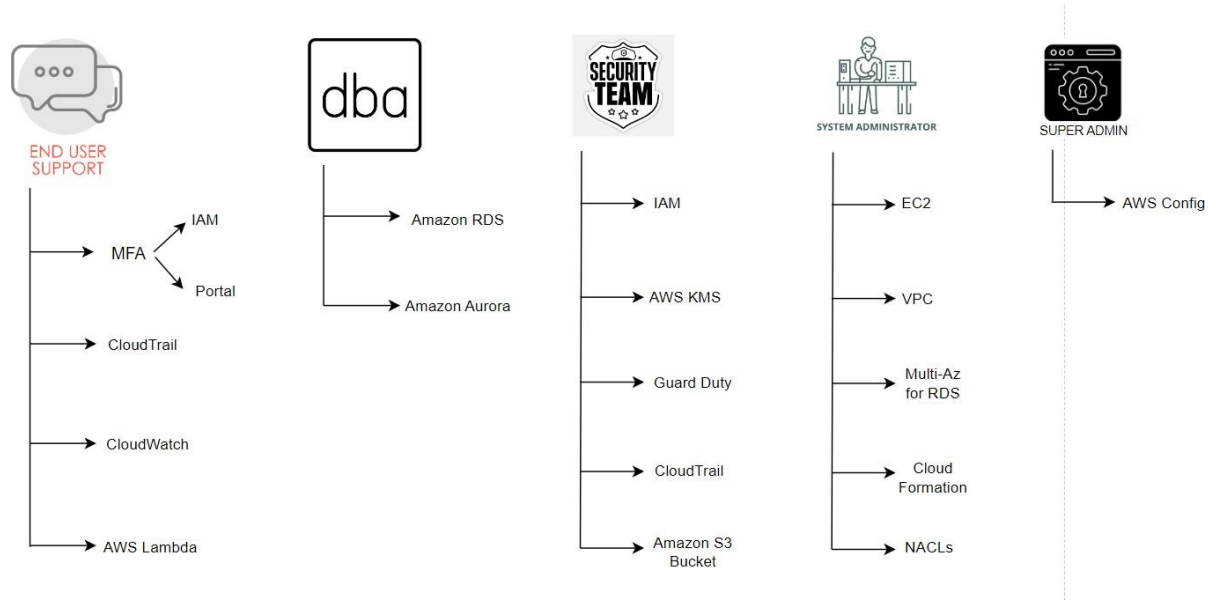
Data Access and Information Management:

The application will allow care providers to manage and access the patient's records. The important focus should be accessing the medical records timely and making them available for viewing, uploading, and downloading, as they need to access the data all the time for emergency reasons. Along with that, care providers need to review and update patients' data ensuring integration with the latest test reports, personal information, medical history, and medical plans. AWS S3 (Simple Storage Service) and Amazon Aurora will help store and secure the data through configuration, encryption, and versioning for automated data. With the help of AWS services, the architecture will help mitigate risks to data integrity.

Third-Party Communication:

For secure communication between care providers, including hospitals, can be employed with the available AWS service. Care providers can securely send and receive messages related to sending test results, information updates, and online consultations. The third-party communication will be handled by a secure API, including the Simple Email Service for email communication. The users will receive notifications through Simple Notification Service via the portal. The incorporation of AWS services will provide healthcare care providers with a secure and robust way of communicating via the infrastructure, along with ensuring patient interactions and information transfer follow the required standards of privacy and regulatory compliance.

Architecture details from an IT Support Point of View:



Img 1.3 Architecture flow from an IT Support Point of View:

End User Support:

The end user support team accesses the infrastructure using IAM credentials with MFA to ensure secure access. Once logged in, they work on AWS Cloud Watch and Cloud Trail to vigilantly monitor and troubleshoot user activities in real-time. They establish a regular communication channel with the end-users via the Amazon SNS notification service. The support team automates the tasks of scheduling appointments on the portal by using the AWS lambda function.

Database Administrator Role:

The database administrators undertake measures to securely access and manage the databases which are hosted on AWS RDS and Amazon Aurora. Next, they focus on timely modification of the database where AWS RDS allows them to process, provide encryption at rest and automate backups with AWS Backup service. They utilize the dynamic capability of Amazon Aurora along with RDS to provide better data integrity and work on developing a stable database which easily adapts to the needs of patients in future as well.

Security Team:

The team works on implementing strict access control using AWS IAM to manage roles, permissions, and policies. Their focus then shifts to encrypting the data with AWS KMS, ensuring sensitive information is guarded properly from unauthorized access. To monitor for potential security threats and anomalies in the infrastructure, they deploy AWS Guard Duty. Further, they establish CloudTrail services for incident response such that the compliance standards are also met. To adhere to HIPAA privacy regulations in healthcare, Amazon S3 is configured for security regulation and awareness of the IT team.

System Administrator:

Sys Admins focus on virtual machine integration and deployment using Amazon EC2, allowing auto-scaling for dynamic resource allocation. They manage the configuration of network settings via Amazon VPC and isolate the security groups using NACLs. Multi-AZ for Amazon RDS helps them in making the system fault tolerant and Cloud Formation allows them to automate the infrastructure easily.

Super Admin Role:

Super Admins control AWS organizations to manage with proper structuring for the multiple AWS accounts used by different IT teams within the infrastructure. After logging in through IAM credentials they create a centralized hub for governance and resource allocation for multiple AWS accounts. They use AWS Config for compliance assessment, and configuration history with heuristic analysis for resource inventory, which helps them in tracking active AWS instances in all regions centrally. AWS Secret manager ensures that all super admins maintain a secure approach in handling the confidentiality of data.

References

https://docs.aws.amazon.com/autoscaling/ec2/userguide/attach-load-balancer-asg.html

https://docs.aws.amazon.com/secretsmanager/latest/userguide/hardcoded.html

https://aws.amazon.com/shield/

https://aws.amazon.com/waf/

https://aws.amazon.com/route53/

https://aws.amazon.com/cloudfront/

https://aws.amazon.com/console/

https://aws.amazon.com/s3/

https://aws.amazon.com/guardduty/

https://aws.amazon.com/pm/cloudwatch/

https://aws.amazon.com/pm/cloudtrail/

https://aws.amazon.com/inspector/

https://aws.amazon.com/systems-manager/

https://aws.amazon.com/security-hub/

https://aws.amazon.com/elasticloadbalancing/

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

https://aws.amazon.com/macie/

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html

https://aws.amazon.com/sns/

https://aws.amazon.com/lambda/

https://aws.amazon.com/config/

https://aws.amazon.com/backup/

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.Keys.html

https://aws.amazon.com/secrets-manager/

https://aws.amazon.com/pm/cognito/