Medcircle Recommended Actions

ENPM-665 Final Project

12/15/2023

Authors: Pranay Venkata Bhamidipati(pbhamid1); Kushangi Nilpeshbhai Patel (kpatel64); James Graves (jgrav008)

Contents

Contents 2
AWS services/components to improve Platform Security [12] 3
SERVICES AND METHODOLOGIES 4
A. Weak Access Controls: 4
B. Unencrypted Data: 6
C. Vulnerable Virtual Machines 7
D. Inadequate Network Security: 8
E. Insufficient Disaster Recovery: 8
F. Lack of Logging and Monitoring: 9
Network Architecture 11
Architecture Diagram from Patient's point of view: 11
Architecture Diagram from Care Provider's point of view: 14
Architecture Diagram from IT Support point: 16
Conclusion 18
References 19
Bibliography 19

AWS services/components to improve Platform Security [12]

- **AWS Single Sign-On with Multi-Factor Authentication (MFA):**
  Implementing AWS Single Sign-On (SSO) with Multi-Factor Authentication (MFA) adds an extra layer of security by requiring users to authenticate themselves using multiple verification methods. This ensures that even if login credentials are compromised, unauthorized access is less likely. [8]
- **Amazon Route 53 DNS:**
  Utilizing Amazon Route 53 for Domain Name System (DNS) management enhances the security and reliability of domain name resolution. It provides features such as DNSSEC (Domain Name System Security Extensions) for protecting against DNS spoofing and cache poisoning attacks.[3]
- **Amazon GuardDuty:**
  Implement Amazon GuardDuty to continuously monitor and analyze AWS account activity for potential security threats and vulnerabilities. GuardDuty uses machine learning to detect malicious activity, unauthorized access, and other suspicious behavior.[1]
- **AWS Shield:**
  AWS Shield is a managed Distributed Denial of Service (DDoS) protection service. It helps safeguard applications and websites from DDoS attacks by automatically detecting and mitigating malicious traffic, ensuring uninterrupted service availability. [4]
- **HTTPS for All Internet Communications:**
  Enforce the use of HTTPS for all internet communications to encrypt data in transit and protect against man-in-the-middle attacks. This involves securing web applications and services with SSL/TLS certificates.
- **AWS Web Application Firewall (WAF):**
  Utilize AWS WAF to protect web applications from common web exploits, such as SQL injection and cross-site scripting. It allows you to define and enforce customizable web security rules. [4]
- **Activate AWS CloudWatch and CloudTrail Logging of Activity:**
  Enable AWS CloudWatch for real-time monitoring and AWS CloudTrail for logging and auditing of AWS account activity. These services provide detailed insights into resource usage, changes, and potential security incidents. [2]
- **AWS Certificate Manager:**

Implement AWS Certificate Manager to manage SSL/TLS certificates easily. It simplifies the process of obtaining, deploying, and renewing certificates, ensuring secure communication between clients and servers. [8]

- **Segregate and Restrict Access to EC2 Web Server and App Servers:** Ensure a clear segregation of duties by restricting access to EC2 web servers and application servers. This involves implementing strict access controls, using security groups and network ACLs to limit communication only to necessary services.
- **Ensure Access Control via User Groups:** Implement access controls through user groups to manage permissions effectively. This ensures that only authorized users, including patients, doctors, and IT support, have the appropriate level of access to sensitive information and system resources.
- **Regular Security Audits and Monitoring:** Conduct regular security audits to identify and address potential vulnerabilities. Implement continuous monitoring to detect and respond to security incidents promptly.
- **Employee Security Training:** Train employees, especially IT support staff, on security best practices and policies. This includes awareness of social engineering threats, password hygiene, and the importance of reporting suspicious activity.

SERVICES AND METHODOLOGIES

Through our architecture design and other recommendations, the most severe security problems that were mentioned in the vulnerability and assessment report would be addressed. The major security problems at a high level are detailed below.

A. Weak Access Controls:

1. Excessive Permissions:

Vulnerability: The IAM user's policy allowing "Action": "s3: *" grants unrestricted control over the S3 bucket, posing a security risk

Recommendations:

- Limiting user rights to the minimum necessary for their tasks can help reduce this risk.
- Implementing strong access controls using IAM policies is advised to protect the S3 bucket's security.
- Impact: Enhances control over the S3 bucket, reducing the potential for unauthorized access and data breaches.

2. Weak Admin and Developer Guidelines:

Vulnerability: Unrestricted policies in the Admin and Developer roles present a serious security risk.

Recommendations:

- Restrict the scope of resources and actions permitted for Admin and Developer roles and put the resources in public and private subnets.
- Minimize the attack surface by following the principle of least privilege in access control.

Impact: mitigates security risks, reducing the attack surface.

3. Users have full access to the S3 bucket:

Vulnerability: users have unrestricted access to the S3 bucket which stores confidential data about the patients.

Recommendation: Implement access controls and restrictions to limit the access permissions for guests to the S3 bucket, ensuring a more secure environment.

Impact: S3 bucket access is restricted.

4. Weak implementation of IAM policies:

Vulnerability: EC2 instances and resources lack defined IAM roles or policies.

Recommendation: Define and assign IAM roles and policies to resources, following the principle of least privilege, for roles such as Patient, Doctor, and IT. According to architecture the roles can be

- Patients can view their health records, appointments etc. But won't be able to access backend infrastructure.
- Care Provider will be able to view, edit, delete the health records of patients, APIs for specific services, but will be given specific levels of permission only. Although, they won't be able to access backend infrastructure, system configuration set by IT support team etc.
- The IT support team would be able to access and edit all system, administrative-related configurations.

Impact: Proper segregation of access level to users

5. Public and Private Security Groups:

Vulnerability: It allows unrestricted access to certain ports within Public and Private Security Groups.

Recommendation: Limit access by specifying IP ranges in security group rules and adhere to the principle of least privilege for better security practices.

Impact: Public and private applications are kept separately and securely.

6. Inadequate Version Control:

Vulnerability: The lack of version control in IAM rules makes tracking changes and upgrades hard.

Recommendation: Specifying version while adding version control improves the management of policies and auditing.

Impact: Enhances disaster recovery as previous version can be restored anytime.

B. Unencrypted Data:

1. SSH Access from InstanceSecurityGroup:

Vulnerability: The InstanceSecurityGroup lets anyone connect via SSH on the internet, which is a security problem.

Recommendation: Allow SSH access from known IP addresses.

Impact: Restricts unauthorized SSH connections from the internet.

2. Unencrypted Data in Transit:

Vulnerability: Without encryption, individuals could read the data being sent between applications.

Recommendation: Use HTTPS connection to and from applications.

Impact: Data in transit is safe from unauthorized access.

3. Unencrypted Data at Rest:

Vulnerability: The RDS database doesn't have any encryption at rest leaving sensitive information in plain sight.

Recommendation: Utilize AWS Key Management Service (KMS) to enable encryption for the RDS instance while it's at rest.

Impact: Data stored in the RDS is safe and secure.

4. Database Access Control:

Vulnerability: The User (DBUsername) and (DBPassword) store database credentials in plaintext within the template, posing a risk.

Recommendation: Utilizing AWS Systems Manager Parameter Store to securely store and manage database credentials.

Impact: Data stored is encrypted and hardcoding of credentials is prevented.

C. Vulnerable Virtual Machines

1. EBS Volume is not encrypted:

Vulnerability: The confidentiality, integrity and availability of data is at risk here. All the sensitive information stored here is at risk and can be compromised.

Recommendation: Usage of AWS Key Management Service (KMS) to encrypt data at rest.

Impact: data within EBS volume is secure.

2. Security group SSH port is open:

Vulnerability: Any individual on the internet can connect to the EC2 instance via SSH connection making it vulnerable to security attacks.

Recommendation:

- Activating CloudWatch Logs and AWS CloudTrail to monitor logs of SSH access.
- Enable AWS Guard Duty to monitor malicious and intrusive activities.

Impact: EBS volume can store sensitive information like patient records and HIPPA data which is now secured.

1. Unrestricted Network Access in Security Groups:

Vulnerability: The lack of traffic restrictions could potentially lead to data disclosure or leakage. Any user within a group can access data across different applications and services within the security group.

Recommendation: Utilizing AWS Virtual Private Cloud (VPC) and subnets enables segmentation, allowing the company's network to be divided into multiple security groups.

Impact: Security groups and subnets segregation for enhanced security.

D. Inadequate Network Security:

1. Default Network Access Control List (NACL):

Vulnerability: The default NACL rule allows unrestricted inbound and outbound traffic. This poses a significant security risk, potentially exposing valuable resources to considerable vulnerabilities.

Recommendation: Identify the necessary outgoing and incoming traffic for the company's services and applications. [13] Based on this, modify the NACL rules to permit only essential traffic while blocking all other types of traffic.
Impact: Prevention of authorized traffic and intrusions.

2. No Flow Logs in subnet:

Vulnerability: Without flow logs illegal activities, intrusions etc., Will be difficult to analyze.

Recommendation: Within a subnet keep flow logs enabled for recording the activities.
Impact: These Flow logs can be stored in log buckets for further digital forensic analysis.

3. VPC Design flaw for future expansion:

Vulnerability: As the infrastructure grows, virtual private clouds (VPC) that do not include strategies for upcoming growth and expansion can have difficulties for resource allocation.

Recommendation:

- Usage of auto scaling groups and keeping EC2 instances there for high demand.
- Load balancers application for dividing traffic inside the infrastructure

Impact: Scaling of applications and services would happen automatically as per demand

E. Insufficient Disaster Recovery:

1. No backup strategy:

Vulnerability: Clearly outlined backup plan covering backup frequency, retention policies, and data types for backup is not present. So, significant risk of data loss is present.

Recommendation: Creation and Implementation of an extensive backup plan that includes backup schedules, retention regulations, and the identification of essential data types.

Impact:

2. Protection against RDS deletion is not enabled:

Vulnerability: Deletion of crucial data by accident is possible. If deleted it is lost forever.

Recommendation: Enabling deletion protection to prevent accidental deletion of data.

Impact: Sensitive records and data are retained as per HIPPA guidelines

3. No Redundancy and Failover Plan:

Vulnerability: The infrastructure lacks redundancy and failover. Without such processes, interruptions or failures in components or services might cause prolonged downtime and loss of access to vital patient data.

Recommendation: Deploy resources and services across a number of different availability zones that are contained inside an area.

Impact: It will enhance the disaster recovery plan by providing a redundancy plan.

F. Lack of Logging and Monitoring:

1. The client system lacked the ability to collect logs from various sources such as audit logs for access, configuration changes, and billing events.

Vulnerability: The client will not have the capability of tracing back unauthorized attempts to access their systems or unauthorized attempts to make changes to their systems.

Recommendations:

1. Activate Amazon CloudWatch.

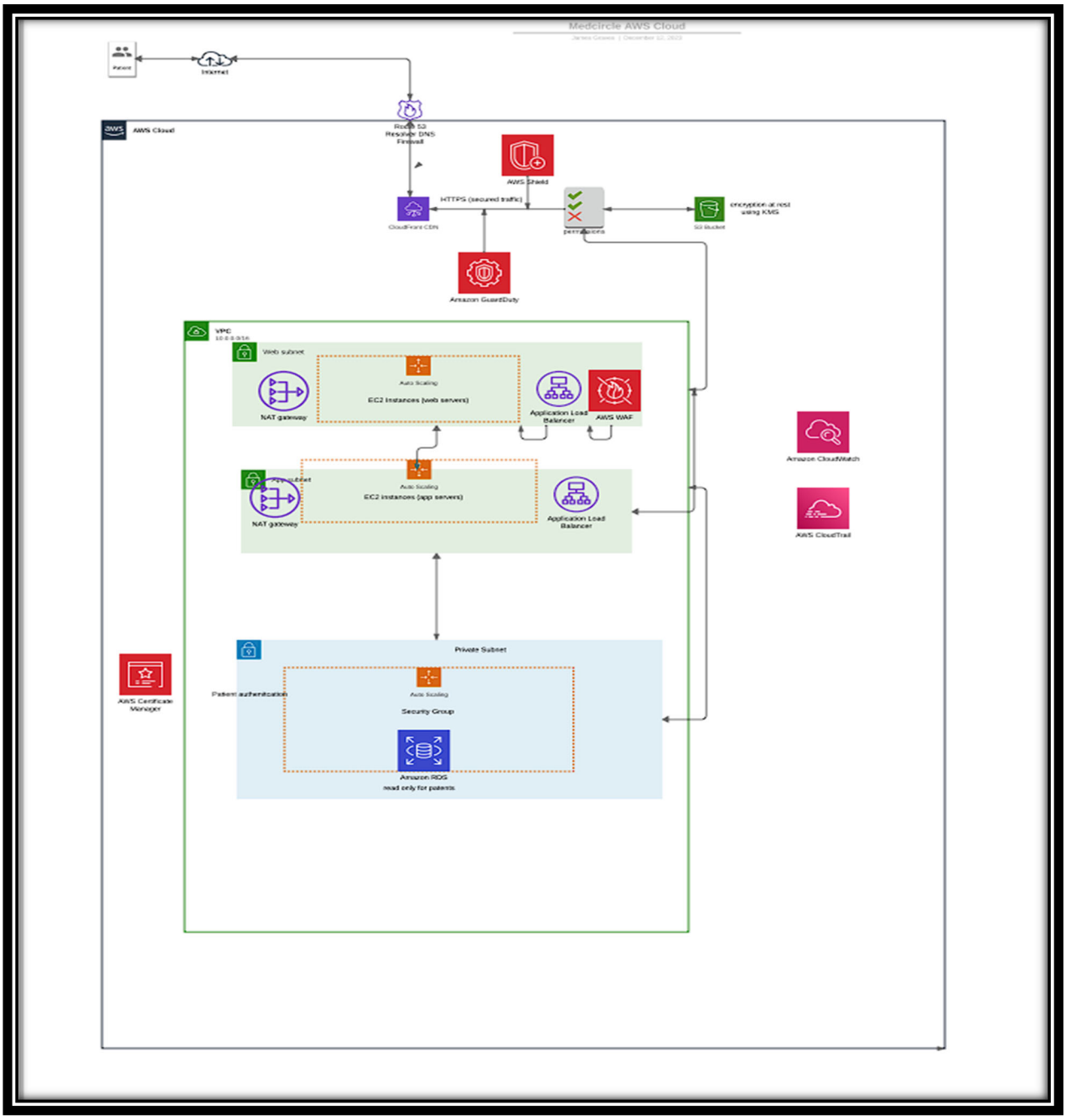
Impact: Amazon CloudWatch consolidates, manages, and analyzes log files from various sources, such as audit logs for access, configuration changes, and billing events. This will improve the client system's ability to track and monitor relevant events. [2]

2. Activate Amazon CloudTrail.

Impact: CloudTrail enables auditing, security monitoring, and operational troubleshooting by tracking user activity and API usage. AWS CloudTrail logs, continuously monitors, and retains account activity related to actions across the client's AWS infrastructure, thus enabling control over storage, analysis, and remediation actions. [9]

Network Architecture

Architecture Diagram from Patient's point of view:



Secure Account Creation and Management:

Upon creating an account on the MedCircle platform, the patient embarks on a journey marked by a secure onboarding process. Personal information is meticulously entered into web forms, protected by advanced encryption and Cross-Site Request Forgery (CSRF) tokens. This ensures that the patient's data remains shielded from any unauthorized access. Passwords undergo advanced cryptographic hashing and storage methods, and the system enforces stringent password policies, fortifying the overall security of the account. Account recovery processes incorporate personal security questions, email or phone verification, and time-sensitive links for password resets – all conducted over secure channels, reinforcing the commitment to protecting sensitive information.

Multifactor Authentication (MFA) and Session Security:

To enhance account security, the patient chooses multifactor authentication during the setup phase. This entails providing a second form of identification, whether a fingerprint or a one-time passcode generated by an authenticator app. This deliberate choice significantly reduces the vulnerability to unauthorized access. After a successful authentication, a secure, time-limited session token is generated, minimizing the risk of session hijacking. The token is securely stored in the patient's browser and is invalidated upon logout or after a period of inactivity, emphasizing the platform's dedication to securing each session.

Encrypted Data Transmission and Protected Health Information (PHI):

Every interaction within the patient portal is characterized by fortified encrypted data transmission. TLS 1.3, with strict policies to prevent downgrade attacks, is employed to ensure the confidentiality of the patient's Protected Health Information (PHI) during transmission. Content security policies are in place to prevent mixed content, mitigating the risk of man-in-the-middle attacks and reinforcing the patient's trust in the security measures implemented.

Telemedicine Consultations and Real-Time Data Exchange:

Telemedicine sessions unfold seamlessly through the implementation of WebRTC-based technologies, featuring end-to-end encryption. This guarantees that only the patient and their healthcare provider can access the video and audio streams, preserving the confidentiality of virtual consultations. Real-time access to Electronic Health Records (EHRs) during consultations is facilitated

through secure and dedicated channels, providing assurance regarding the integrity and privacy of the patient's medical information.

Patient Data Storage and Access:

The patient's data finds a secure home in databases encrypted with AES-256 standards. Access to these databases is meticulously controlled through Identity and Access Management (IAM) roles, adhering strictly to the principle of least privilege. This ensures that only necessary systems and authorized personnel have access. All database queries are parameterized to prevent SQL injection attacks, and access logs undergo regular audits to detect any signs of suspicious activity, underscoring the commitment to maintaining data integrity.

Patient Portal Functionality and Interaction:

When engaging with functionalities like accessing test results or scheduling appointments, the patient interacts with serverless functions, such as AWS Lambda. These functions process requests without persistent server connections, effectively reducing the potential attack surface. Documents or test results transmitted through the platform are secured by a document exchange system that employs encryption and digital signatures, adding an extra layer of assurance regarding the integrity and authenticity of these critical documents.

Proactive Security Measures and Continuous Monitoring:

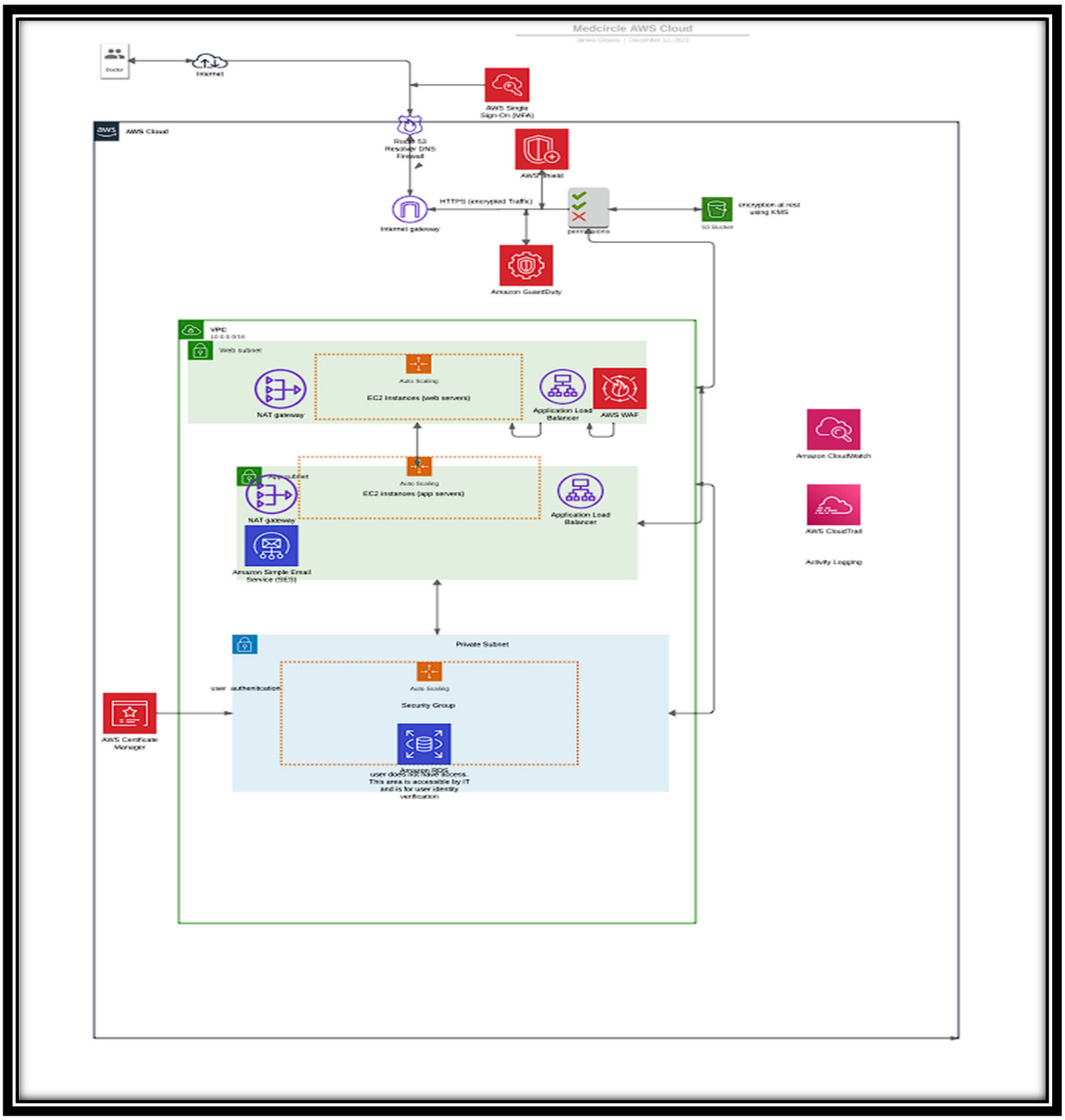
The MedCircle platform extends its commitment to security beyond the initial setup. Proactive measures, including regular vulnerability scanning, penetration testing, and the deployment of Web Application Firewalls (WAFs), are in place to detect and prevent potential exploitation attempts. Real-time monitoring through Security Information and Event Management (SIEM) systems aggregates and correlates logs, providing immediate alerts on potential security incidents. This continuous vigilance reinforces the platform's dedication to maintaining a resilient security posture.

Compliance and Regular Audits:

Adherence to healthcare compliance standards, notably HIPAA, is a guiding principle ensuring that every facet of the platform aligns with regulatory requirements. Regular audits, conducted by independent reviewers, assess the platform's security posture, ensuring continuous improvement and adaptation to

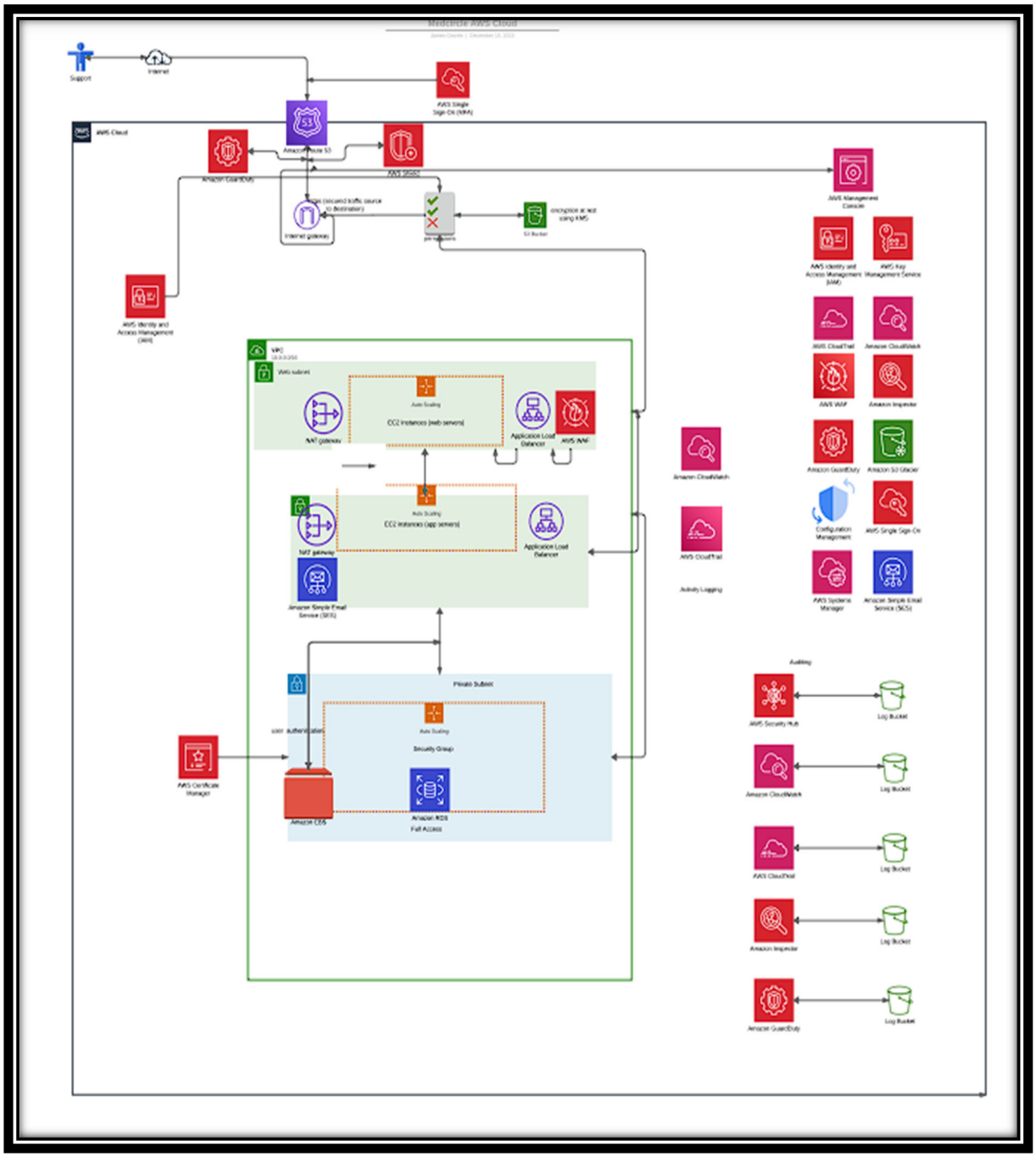
emerging threats. These audits serve as a testament to the platform's commitment to maintaining the highest standards of security and compliance. In conclusion, the patient's interaction with the MedCircle platform is characterized by a multi-layered security strategy that spans the entire data lifecycle. From the moment of account creation to real-time consultations and data storage, the platform offers assurance that sensitive health information is handled with the utmost security and care.

Architecture Diagram from Care Provider's point of view:



- Accessing the hospital's website initiates a process that is secure and efficient. The request made by a doctor is directed through AWS Route 53, a Domain Name Server (DNS) acting as an address locator for the website. Additionally, AWS Shield is present to prevent any DDOS attacks.
- Before gaining access, the doctor's identity undergoes verification, ensuring a secure entry point through the AWS Single-Sign-On (SSO) mechanism, complemented by Multi-Factor Authentication (MFA). These security measures guarantee that only authorized personnel proceed.
- Once inside the system, traffic management is organized. Incoming requests are distributed using load balancers, enhancing system reliability by efficiently handling varying traffic volumes. Moreover, the system's capability to establish connections with doctors is regulated, preventing any external access, this control is provided by Network Address Translation (NAT) services.
- Within the public subnet, the Web Application Firewall (WAF) monitors potential web-based threats. It protects the system from malicious attacks such as SQL Injection or Cross-Site Scripting.
- Communication channels, both within the system and between servers and databases, are safeguarded using Transport Layer Security (TLS) as traffic is transmitted over HTTPS on port 443. The certificates for these security measures are provided by AWS Certificate Manager. This security implementation guarantees confidentiality and integrity among shared information. Further, the public and private subnets are differentiated. The public subnet holds the load balancer, web application firewall. The private subnet is accessible only by the IT support team.
- After verification and based on the permissions, the doctor may view patient records from a secure database using a web server and edit and view data stored in an encrypted S3 bucket. Additionally, Amazon Simple Email Services (SES) is used for communication purposes.
- To provide an additional level of safeguarding, the S3 bucket employs encryption using Key Management Service (KMS) to secure sensitive data, therefore strengthening the security of patient information. Further the Amazon RDS which is used for the application in public subnet is kept secure in the private subnet.
- Activity logging is enabled by AWS CloudWatch which provides real time monitoring of the resources and Amazon CloudTrail provides insights and data for resource management.

Architecture Diagram from IT Support point:



- The IT support team is very important for keeping the AWS system running effectively and securely. They have access to a variety of tools and services to authenticate users, monitor the infrastructure and keep private data safe.
- The identities of IT support staff are checked before they can log in. This is done through the AWS Single-Sign-On (SSO) system and is backed up by Multi-Factor Authentication (MFA). This lets IT support staff use AWS Route 53 to get to both public and private subnet applications. It also acts as a guide to get to different services and apps through the internet gateway. Additionally, AWS Shield is present to prevent any DDOS attacks.
- Identity and Access Management (IAM) is present because it lets the team keep an eye on user permissions and make sure that only authorized people can access AWS resources.
- Within the AWS Management Control, various components include:

    - **AWS IAM-** It is responsible for overseeing access to AWS resources and regulating user privileges and security configurations in the cloud infrastructure. [11]
    - **The AWS Key Management Service (KMS):** It is used for the creation and management of encryption keys used to protect data stored in various AWS services and applications. [10]
    - **AWS WAF:** It actively monitors and prevents possible web-based attacks, such as SQL Injection or Cross-Site Scripting, from compromising the system. [4]
    - **Amazon Inspector:** It evaluates application security and compliance by examining security vulnerabilities and departures from established standards. [5]
    - **Amazon Guard Duty: This** is a service that identifies and detects potential dangers and questionable actions in AWS settings. It also provides alerts to notify the IT support team. [1]
    - **Amazon S3 Glacier:** It offers cost-effective, extended data storage for backup and compliance purposes. It allows recovery of data within a certain timeframe. [6]
    - **Amazon Configuration Management: It** is a system that monitors and maintains the settings of AWS resources. Its purpose is to ensure compliance and security by tracking changes. [11]
    - **AWS Systems Manager:** It streamlines administration by providing automation, resource management and configurations.
    - **AWS Simple Email Service (SES):** It enables seamless sending and receiving of emails between different applications within the

infrastructure.

- Incoming requests are distributed using load balancers, enhancing system reliability by efficiently handling varying traffic volumes. Within the public subnet, the Web Application Firewall (WAF) monitors potential web-based threats. It protects the system from malicious attacks such as SQL Injection or Cross-Site Scripting. Implementation of Network Access Translation (NAT) is done to segregate various EC2 instances.
- Communication channels, both within the system and between servers and databases, are safeguarded using Transport Layer Security (TLS) as traffic is transmitted over HTTPS on port 443. The certificates for these security measures are provided by AWS Certificate Manager. [8] This security implementation guarantees confidentiality and integrity among shared information. Further, the public and private subnets are differentiated.
- Access to patient data undergoes strict verification and is managed via IAM policies. Extra security layers, such as encryption using Key Management Service (KMS), increases the protection of patient information stored in the S3 bucket. Moreover, Amazon RDS applications in the public subnet are securely housed within the private subnet. Further, Amazon EBS is securely kept in the private subnet which cannot be accessed by the Patient and Care provider.
- Additionally, logging and monitoring services like Amazon CloudWatch, AWS Security Hub, Amazon Guard Duty, AWS CloudTrail, and Amazon Inspector record traffic flow and activities, storing logs in designated log buckets for detailed security analysis by the IT support team. [4]

Conclusion

Upon review of the Medcircle's AWS cloud-based platform and undertaking performance testing as requested, several vulnerabilities were identified that require corrective action to ensure the adequacy of Medcircle's cybersecurity controls. For each of the vulnerabilities identified, recommended actions have been provided that, if implemented as described in this document, will help ensure the security of Medcircle's AWS cloud based medical platform.

References

Bibliography

1. Amazon Documentation. (2023, 12 14). *AWS Documentation*. Retrieved from AWS GuardDuty: https://aws.amazon.com/guardduty/
2. Amazon Documentation. (2023, 12 2023). *Management and Governance*. Retrieved from Amazon CloudWatch: https://aws.amazon.com/cloudwatch/
3. Amazon Documentation. (2023, 12 11). *Network and Content Delivery*. Retrieved from Amazon Route 53: https://aws.amazon.com/route53/
4. AWS Developer Guide. (2023, 12 11). *AWS WAF, AWS Firewall Manager and AWS SHIELD ADVANCED*. Retrieved from AWS Developer Guide: https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html
5. AWS Documentation. (2023, 12 11). *Amazon Inspector*. Retrieved from AWS Documentation: https://aws.amazon.com/inspector/
6. AWS Documentation. (2023, 12 11). *Amazon S3 Glacier*. Retrieved from AWS Documentation : https://aws.amazon.com/pm/s3-glacier/?gclid=CjwKCAiApuCrBhAuEiwA8VJ6JkvY287IAbE86hprtCMIENN7M3zcAdTRnjGzsEFHElhGYNBTNdBx5hoCWCMQAvD_BwE&trk=20e04791-939c-4db9-8964-ee54c41bc6ad&sc_channel=ps&ef_id=CjwKCAiApuCrBhAuEiwA8VJ6JkvY287IAbE86hprtCMIENN7M3zcAdTRnj
7. AWS Documentation. (2023, 12 11). *Amazon VIrtual Private Cloud*. Retrieved from User Guide: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html
8. AWS Documentation. (2023, 12 11). *AWS Certificate Manager*. Retrieved from aws Dcoumentation: https://aws.amazon.com/certificate-manager/
9. AWS Documentation. (2023, 12 11). *AWS CloudTrail*. Retrieved from AWS Documentation: https://aws.amazon.com/pm/cloudtrail/?gclid=Cj0KCQiAj_CrBhD-ARIsAIiMxT9Kcly0QD-7ahxopu8XLAeBDndVx_jHTp9X3F-pfWcYcud0jZ0P7mIaAluaEALw_wcB&trk=f6e79447-9b4c-4310-8415-1a76de2de47f&sc_channel=ps&ef_id=Cj0KCQiAj_CrBhD-ARIsAIiMxT9Kcly0QD-7ahxopu8XLAeBDndVx_jHT
10. AWS Documentation. (2023, 12 11). *AWS Key Management Service*. Retrieved from Aaws: https://aws.amazon.com/kms/

11. AWS Documentation. (2023, 12 11). *AWS Systems Manager*. Retrieved from AWS Documentation: https://aws.amazon.com/systems-manager/

12. AWS Documentation. (2023, 12 11). *AWS Whitepaper*. Retrieved from AWS Cloud Adoption Framework: Operations Perspective: https://docs.aws.amazon.com/whitepapers/latest/aws-caf-operations-perspective/configuration-management.html

13. Newsroom. (2023, 12 11). *The Hacker News*. Retrieved from New OpenSSH Vulnerability Exposes Linux Systems to Remote Command Injection: https://thehackernews.com/2023/07/new-openssh-vulnerability-exposes-linux.html