SECURE CLOUD INFRASTRUCTURE

(Assignment 2 – Internee.pk)

1. Introduction

A crucial component of contemporary IT architecture is cloud computing. Cloud platforms are used by businesses to host apps, store data, and provide services all over the world. Although cloud platforms offer scalability and flexibility, they also present additional security risks such misconfigurations, illegal access, data breaches, and web-based assaults.

To guarantee data availability, confidentiality, and integrity, cloud infrastructure security is essential. The implementation and evaluation of industry-standard security procedures in a cloud environment are the main objectives of this assignment. Amazon Web Services (AWS) was chosen as the cloud platform for this project because of its industry acceptance and extensively used security services.

2. Objective of the Task

Ensuring cloud-based infrastructure adheres to industry-standard security standards is the primary goal of this assignment. The particular objectives of this work consist of:

Using Identity and Access Management (IAM) to audit cloud access and permissions
Using security logs to keep an eye on cloud activity
Using redundancy and backups to ensure data security
Using an online Application Firewall (WAF) to shield online applications from outside threat
Knowing how AWS Open Data is used to securely hold public cloud data

This assignment offers hands-on experience with cloud security principles that are frequently applied in actual business settings.

3. Cloud Platform Overview (AWS)

One of the top cloud service providers is Amazon Web Services (AWS), which provides a variety of security-related services. AWS employs a shared responsibility paradigm in which clients are in charge of protecting their data, access controls, and configurations while AWS secures the underlying cloud infrastructure.

AWS offers integrated services for:
Management of identity and access
Monitoring and recording activities
Encryption and backup of data
Security of networks and applications

Because of these characteristics, AWS can be used for cloud security control implementation and auditing.

4. IAM Security Audit (Identity and Access Management)

One of the most crucial security elements in any cloud environment is Identity and Access Management (IAM). IAM regulates who has access to cloud resources and what they can do.

The IAM configuration was examined in this process to make sure:
The root account is not utilized for regular activities and is protected.
Rather than employing the root account, IAM users are created.
Policies are used to assign permissions.
Users only get the permissions they require because the least privilege principle is adhered to.

The risk of unwanted access and unintentional exploitation of cloud resources is greatly decreased by verifying IAM settings.

5. Cloud Security Logging (AWS CloudTrail)

Monitoring cloud activities is crucial for conducting security audits and identifying questionable activity. AWS offers a feature called AWS CloudTrail, which keeps track of all account activity.

CloudTrail logs consist of:
Attempts by users to log in
Calls to APIs
Events involving the development and destruction of resources
Modifications to the configuration

CloudTrail was enabled to track cloud activity across regions for this task. Security teams use these logs to look into issues, find unauthorized activity, and keep security standards up to date.

6. Data Backup and Redundancy

Data protection is a key component of cloud security. In cloud environments, data loss can occur due to accidental deletion, misconfiguration, or service outages. To mitigate these risks, backup and redundancy mechanisms are required.

In this task, **Amazon S3** was explored as a data storage and backup solution. The concept of **multi-region backups** was studied, where data is replicated across multiple geographical regions. This ensures:

- High availability
- Disaster recovery
- Business continuity in case of region failure

Implementing backups and redundancy helps protect critical data from permanent loss.

7. Web Application Firewall (WAF)

Web applications are common targets for cyber attacks such as SQL injection and cross-site scripting (XSS). To protect applications from such threats, a Web Application Firewall is used.

In this task, **AWS WAF** was explored. AWS WAF allows organizations to:

- Filter incoming web traffic
- Block malicious requests
- Apply managed security rules
- Protect applications from common web-based attacks

Using a WAF adds an extra layer of protection between external users and cloud-hosted applications.

8. AWS Open Data (Public Cloud Datasets)

AWS Open Data was explored to understand how large public datasets are securely hosted in the cloud. AWS Open Data provides openly available datasets for research, education, and innovation.

Although the data is public, it is still hosted on secure cloud infrastructure with proper access controls, logging, and monitoring. Exploring AWS Open Data helped in understanding that cloud security practices apply not only to private data but also to public datasets at scale.

9. Security Best Practices Observed

During this task, several cloud security best practices were observed:

- Avoid using the root account for daily activities
- Use IAM policies with least privilege
- Enable logging and monitoring services
- Implement regular backups and redundancy
- Use WAF to protect applications from external threats

These practices are commonly used in enterprise cloud environments to reduce security risks.

10. Conclusion

This task provided hands-on understanding of securing cloud infrastructure using industry-standard security measures. By auditing IAM configurations, enabling CloudTrail logs, exploring data backups, implementing WAF protection, and reviewing AWS Open Data, key cloud security concepts were successfully covered.

The task helped in understanding how organizations secure cloud platforms against unauthorized access, data loss, and external attacks. Overall, this assignment strengthened practical knowledge of cloud security and its importance in modern IT environments.