Cloud Security Implementation Report for Task 4 of your internship.

Cloud Security Implementation Report

Internship Task - 4

Platform Used:Amazon Web Services (AWS

Objective

The objective of this task is to implement essential cloud security measures on a cloud platform by configuring IAM policies, securing storage, and enabling data encryption. This ensures data privacy, controlled access, and protection against unauthorized access or breaches.

Cloud Platform: AWS (Amazon Web Services)

IAM Policies Configuration

Actions Performed:

Created IAM Users with limited permissions.

Defined IAM Groups for better access control.

Attached pre-defined AWS managed policies:

AmazonS3FullAccess

AmazonEC2ReadOnlyAccess

Enabled MFA (Multi-Factor Authentication) for users.

Created custom IAM policies

Storage (S3 Bucket)

Bucket Configuration:

Bucket Name: secure-bucket

Blocked all public access

Enabled versioning to retain previous versions

Configured access logging to monitor access patterns

Bucket Policy Snippet:

Data Encryption

Encryption at Rest:

Enabled Server-Side Encryption using AWS KMS

KMS key used: alias/aws/s3

Encryption in Transit:

Ensured all access to the bucket is via HTTPS

Denied access over HTTP using bucket policies

Testing and Validation

Verified restricted access using IAM roles

Tested bucket upload/download over HTTPS

Attempted public access (received Access Denied as expected)

Checked versioning by uploading multiple versions of a file

Conclusion

The cloud security setup was successfully implemented using AWS. IAM policies now enforce limited access, S3 storage is secure with encryption and versioning, and sensitive data is protected both in transit and at rest.