e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:11/November-2022 Impact Factor- 6.752 www.irjmets.com

CLOUD SECURITY WITH AWS

Abhijit Mali*1, Shailesh Bendale*2

*1Student, Department Of Computer Engineering, NBN Sinhgad School Of Engineering Pune Maharashtra India.

*2Professor And Head Of Department Computer Engineering, NBN Sinhgad School Of Engineering Pune Maharashtra India.

DOI : https://www.doi.org/10.56726/IRJMETS30997

ABSTRACT

Cloud computing is a modern method of computing in the field of computer science. A collection of resources and services known as "cloud computing" are provided by a network or the internet. New techniques are emerging as the field of cloud computing expands. The environment for cloud computing is expanding, which presents new security difficulties for cloud developers. Because cloud users save their data there, a lack of security in the cloud may undermine user confidence. The best part about cloud security is that it not only safeguards data, especially PII (personally identifiable information) like SSNs, bank account numbers, passport numbers, and so forth, but also applications that access the data. Even the infrastructure (such as servers) on which apps are running is protected by cloud security. Amazon Web Services (AWS) delivers a scalable cloud computing platform with reliability ..offering the resources necessary for users to operate a variety of apps. The security, integrity, and availability of our customers' systems and data, as well as preserving their trust and confidence, are of the utmost importance to AWS. In This paper we are going to understand and learn about cloud security with aws , how aws providing security to its underlying customers and tools and services provided by aws .at the end we will learn how can we secure S3 Storage Buckets.

Keywords: Cloud Computing, Cloud Security, Aws, S3.

I. INTRODUCTION

Delivery of IT resources over the internet is known as cloud computing. The cloud is similar to a virtual data centers that you can access online and allows you to manage storage services for data and applications including databases, servers, networking, analytics, artificial intelligence, security services, etc. Companies that provide network services, infrastructure, or commercial applications in the cloud are known as cloud service providers (CSPs). Several instances of widespread cloud service providers include: Google Cloud Platform (GCP), Microsoft Azure, Amazon Web Services (AWS), etc. The goal of cloud security is to protect cloud environments, cloud-based applications, and cloud-stored data. Cloud security is a collection of technologies, protocols, and practice guidelines. Both the provider and the consumer are responsible for cloud security. The most popular cloud providers are Amazon Web Services (AWS), Azure Cloud, and Google Cloud Platform (GCP) follows the shared responsibility model.

Security in cloud computing varies depending on the types of services used, such as public, private, and hybrid clouds. Software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service are examples of public cloud services run by a public cloud provider (PaaS).

A computer environment specific to one customer is provided by private cloud services provided by public cloud providers. internal staff-operated private cloud services Private and public cloud computing setups are mixed in hybrid cloud services. Internal staff is involved, as well as possibly a public cloud provider.

II. AWS SECURITY

Everyone wants total control and the assurance that comes with using the most versatile and secure cloud computing environment currently available. AWS is a cloud computing platform that helps in the development of your cloud-based apps . In addition to computing power, scalability, stability, and secure database storage, it provides a variety of services including infrastructure and software services. AWS offers about 200 products and services globally, so you can use it for high-quality development.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:11/November-2022 Impact Factor- 6.752 www.irjmets.com

Shared Security Responsibility Model

Security in the cloud is slightly different than security in your on-premises data centers. When you move computer systems and data to the cloud, security responsibilities become shared between you and your cloud service provider.

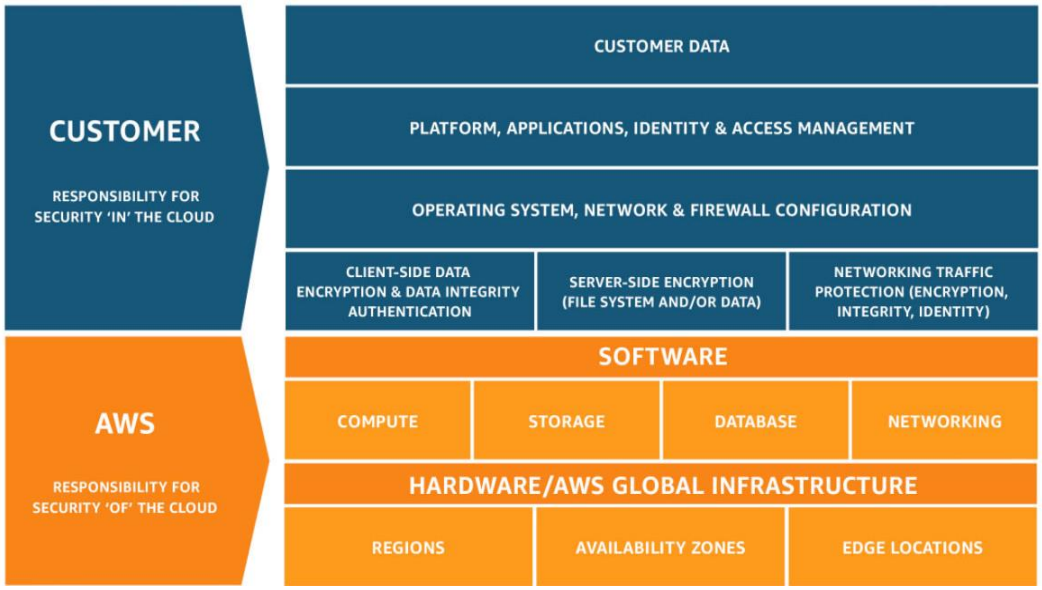


Figure 1: AWS shared Resposibility Model.

Security in the cloud is the responsibility of the customer, and security in the cloud is the responsibility of AWS.

Responsibility of AWS: Protecting the infrastructure that underlies all of AWS's services is entirely under its control. In other words, starting with the host operating system and virtualization layer all the way down to the physical layer, AWS maintains, runs, and controls every part of the service..

Customer Responsibility: The customer is accountable for making sure that the AWS service they are using is setup securely. In other words, guests' operating systems, software upgrades, and application software must be managed by customers. Additionally, they must establish the restrictions imposed supplied by AWS, such as security groups and network access and IAM

Depending on the service used, AWS and the clients may each have a different level of responsibilities.

III. AWS SECURITY FUNDAMENTALS

AWS Security tools are categorized into six core components

1. Identity and Access Management

Users, Groups, and Policies are a few of the fundamental elements of IAM. You can interact with AWS by creating an instance called an IAM user in AWS. This could be a user who is a real person or it could be a user who is an application. An IAM group is a set of IAM users. IAM groups can be used to specify permissions for a number of users. Access to AWS resources is governed by IAM policies, which define permissions. In AWS, policies are recorded as JSON documents.

Tools used for Identity and Access Management in AWS Are

- **Amazon Cognito**

Amazon Cognito provides identity and sync services for mobile and web-based applications. It simplifies the task of authenticating users and storing, managing, and syncing their data across multiple devices, platforms, and applications .Your users can sign in directly with a user name and password, or through a third party, such as Amazon ,Apple, Facebook, or Google.

- **Security Token Service**

AWS Security Token Service is an AWS service that allows you to request temporary security credentials for your AWS resources

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:11/November-2022 Impact Factor- 6.752 www.irjmets.com

2. Detective Controls

You can detect a potential security flaw, threat, or odd behavior through detection. It is a crucial component of the security lifecycle and can be used to support a quality standard, a legal or compliance obligation, as well as efforts to identify and respond to vulnerabilities.

Tools used for Detection Control Are :

- **AWS CloudTrail**

An AWS service auditing tool is called AWS CloudTrail. Your AWS account's API call history is saved. to make it simple for you to trace unwanted access to your AWS account. For your AWS account, CloudTrail logs and records a history of API calls. You can use this information to troubleshoot operational issues, monitor compliance with corporate policies, and track recent changes to your Aws account.

- **AWS Cloudwatch**

The AWS Cloudwatch service monitors all aspects of the AWS platform, including databases, storage, computing, and other services. Users can gain system-wide visibility into resource use, application performance, and operational health thanks to this monitoring solution. These insights might help you react and maintain the efficiency of your application

3. Infrastructure Protection

Infrastructure protection includes the control techniques, such as defence in depth, required to satisfy organisational or legal requirements as well as best practices. For successful, ongoing operations, whether in the cloud or on-premises, these approaches must be used.

Using either native AWS technologies or third-party products and services available through the AWS Marketplace, stateful and stateless packet inspection can be implemented in AWS. Use Amazon Virtual Private Cloud to create a safe, private, and scalable environment where you can describe your topology, including gateways, routing tables, and public and private subnets (Amazon VPC).Aws System manager, cloud-formation, direct connect are few of tools used for infrastructure protection.

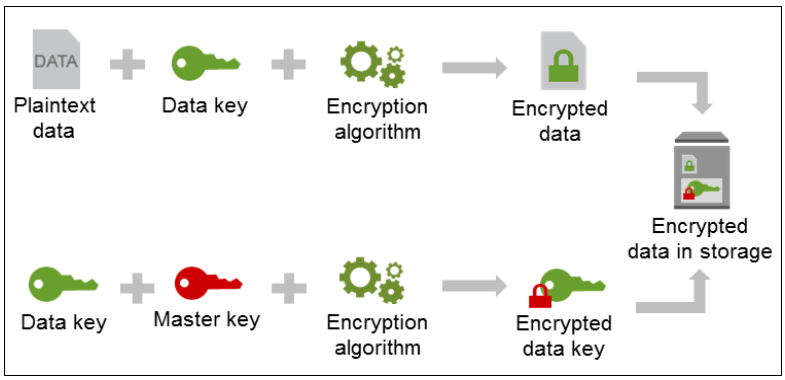
4. Data Protection

Everyone is extremely concerned about data security. And every day, its significance increases. AWS is aware of this and offers a number of measures to protect the data. The world's largest data store might be S3. The security of data saved on S3 greatly depends on encryption. For this data, AWS offers us several encryption methods from which we can select the one that best fits our needs.

In AWS there are several tools that provide data protection:

- **AWS Key Management Service**

With the use of a Customer Master Key (CMK) on the AWS cloud, we may encrypt and decrypt our data using the AWS Key Management Service (AWS KMS). One of the most important services for protecting your AWS account and all of its data is AWS Key Management Service (AWS KMS). KMS offers security that must be implemented before new services and data are received. It is great practices to set up KMS keys before beginning other AWS services like EC2, S3, Cloudtrail , Lambda, and so forth because many other AWS services will require them.



e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:11/November-2022 Impact Factor- 6.752 www.irjmets.com

Fig 2: KMS Encrypt Data process

5. Incident Response

An incident response process is a collection of procedures aimed at identifying, investigating and responding to potential security incidents in a way that minimizes impact and supports rapid recovery. every business should have an incident response plan to be able to take action at any time.

AWS provides several tools and methods for incident response

- **AWS Incident Manager**

You can plan, organise, and keep track of incidents with the aid of AWS Incident Manager, a cloud-based incident management solution. It gives you a unified view of all of your AWS resources and makes it easier for you to handle incidents and take appropriate action.

- **AWS Event Bridge**

Using information from your AWS resources, AWS Event Bridge is a serverless event bus that makes it simple to link apps. Event Bridge can be used to process and filter events, spread out events to numerous targets, and route events to various targets based on the event data. You can use Event Bridge to process events from AWS services like Amazon S3, Amazon DynamoDB, Amazon Kinesis, and Amazon CloudWatch as well as your own programmes and services because it is accessible in all public AWS Regions.

6. DDoS Mitigation

The technique of successfully defending a targeted server or network from a distributed denial-of-service (DDoS) attack is known as DDoS mitigation. A targeted victim might lessen the hazard by using specialised network hardware or a cloud-based protection service.

Aws provides a security approach to avoiding DDoS attacks. tools can be used for this:

- **AWS Shield**

Elastic Load Balancers, CloudFront distributions, and Amazon Route 53 hosted zones are all protected from DDoS attacks by AWS Shield Comprehensive**.**

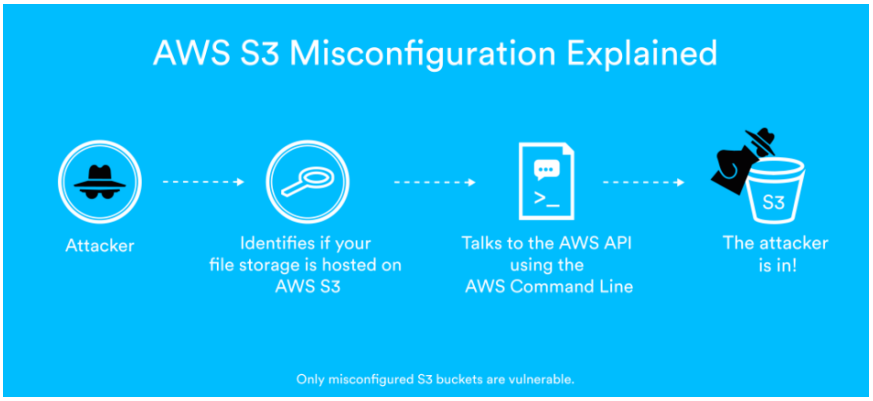
- **AWS WAF**

Web (HTTP/HTTPS) request monitoring for Aws Cloud service distributions and application load balancing are features of the web application firewall service known as AWS WAF. With the help of customizable Rules, you can filter online traffic, block dangerous requests, and evaluate and improve your web apps.

IV. S3 SECURITY

AWS's (Amazon Web Services) S3 [Amazon Simple Storage Service] buckets are a type of publicly available cloud storage that provide scalability, data availability, security, and performance. S3 can store practically any kind of data, in any format. The volume and number of things that can be stored in S3 are both boundless in terms of capacity. In S3, an object is the basic unit of establishment. Data, keys, and metadata make up this object. S3 buckets can also be categorized as private or public.

Most of time s3 bucket are misconfigured because of s3 policies and poor encryption. If your s3 buckets are Misconfigured, attackers could get full access to your S3 bucket, allowing them to download, upload and overwrite files.



e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:11/November-2022 Impact Factor- 6.752 www.irjmets.com

Fig 3: AWS s3 Misconfiguration

- **Checking for vulnerable S3 Bucket**

To check for S3 bucket misconfiguration in security researcher's perspective ,you need to perform some steps

1. Make AWS Account and install AWS CLI on your local system.

2. The following URL enables us to communicate with the AWS S3 bucket.

http://[bucketname].s3.amazonaws.com/

3. To Checking for Misconfigured / vulnerable AWS S3 Bucket

Command: aws s3 ls s3://[bucketname]

Now following are few commands you can try on AWS Bucket via AWS CLI to check whether bucket is vulnerable or not . if bucket is buggy then you can upload delete data from bucket via aws cli

If the following commands return "AccessDenied" errors, it means that the bucket does possess the appropriate ACLs (Access Control Lists) for either the buckets or the objects.

Command	Description
aws s3 ls s3://[aws-bucket-name] --no-sign-request	lists a bucket's contents. It ought to list every item and prefix in the bucket.
aws s3 mv yourfile s3://[aws-bucket-name]/hack.txt --no-sign-request	To move a file or object, use s3 mv. A local file or S3 object can be moved to another location remotely or in S3 using the s3 mv command.
aws s3 rm s3://[aws-bucket-name]/file.svg	S3 rm command can be used to remove a file from an S3 bucket.

- **How to fix it**

Change privileges on your bucket. Amazon S3 offers access policy options broadly categorized as resource-based policies and user policies. Access policies that you attach to your resources (buckets and objects) are referred to as resource-based policies.

V. CONCLUSION

We concluded this paper with all the security measurements taken with AWS to make it secure and better. In this paper, we successfully study all the tools and security methods provided by AWS to make better clouds. Along with this, initially, we learned about how the cloud responsibility model works, and at the end of the paper, we did research on S3 buckets to understand it in depth and learned about techniques to identify misconfigured S3 buckets.

VI. REFERENCES

[1] https://docs.aws.amazon.com/pdfs/wellarchitected/latest/security-pillar/wellarchitected-security-pillar.

[2] https://docs.aws.amazon.com/AmazonS3/latest/userguide/s3-access-control.html.

[3] Michael Soltys,"Cybersecurity in the AWS Cloud" ,Cryptography and Security (cs.CR) arXiv:2003.12905

[4] https://blog.detectify.com/2017/07/13/aws-s3-misconfiguration-explained-fix/