MANIPAL UNIVERSITY
JAIPUR
(University under Section 2(f) of the UGC Act)

A+ NAAC

ICICV

Springer

3rd International Conference on Innovations in Computational Intelligence and Computer Vision

ICICV-2022

November 24-25, 2022

Securing a SaaS Application on AWS Cloud

Presented By:

Siddhartha Sourav Panda

Nishanth Kumar

Dr. Shinu Abhi

REVA Academy for Corporate Excellence (RACE), REVA University, Bangalore

REVA
UNIVERSITY
Bengaluru, India
Established as per the section 2(f) of the UGC Act, 1956,
Approved by AICTE, New Delhi

Paper ID: 225

Outline

- Introduction
- Literature Review
- Problem Statement
- Objectives
- Architecture Diagram
- Implementation
- Testing and Validation
- Analysis and Results
- Conclusion and Future Scope
- References

Introduction

- In recent years, there has been tremendous growth in cloud adoption where companies and startups are embracing cloud technologies to avoid the on-premises costs of maintaining the systems.
- As organizations grow and continue to invest in digital transformation, the cloud is becoming an ever more crucial part of the organization.
- Cyber and ransomware attack attempts on the cloud have been increasing every year.
- The cloud consists of a multitude of settings, policies, assets, and interconnected services and resources, making it a highly sophisticated environment.
- Migration to the cloud is not as easy as it seems when there is a complexity and lack of understanding of baseline and multiple security aspects of the architecture.

Introduction Contd.

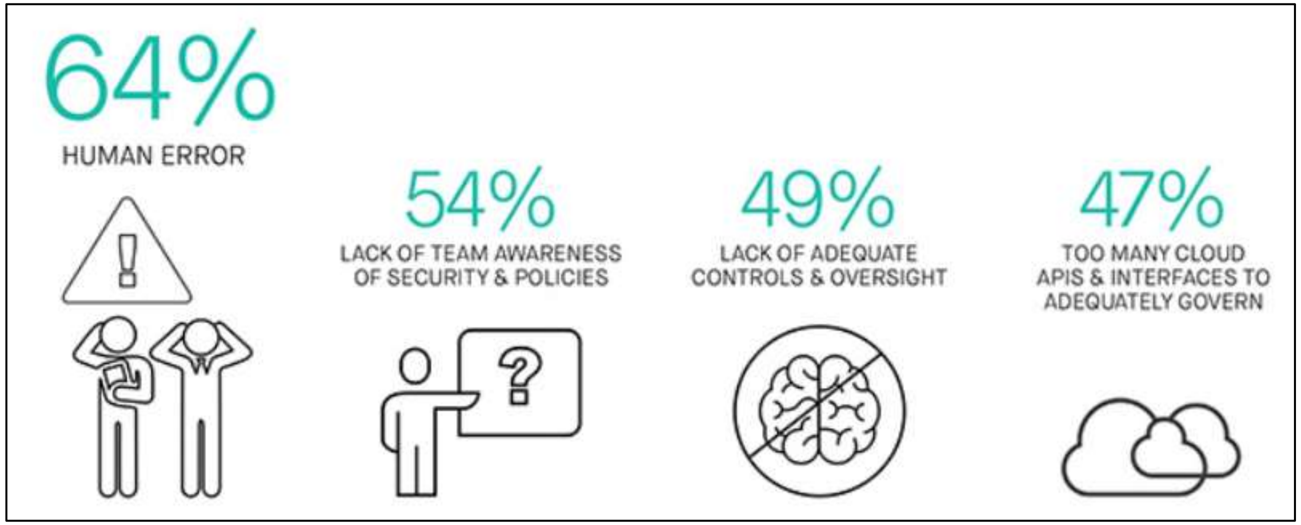
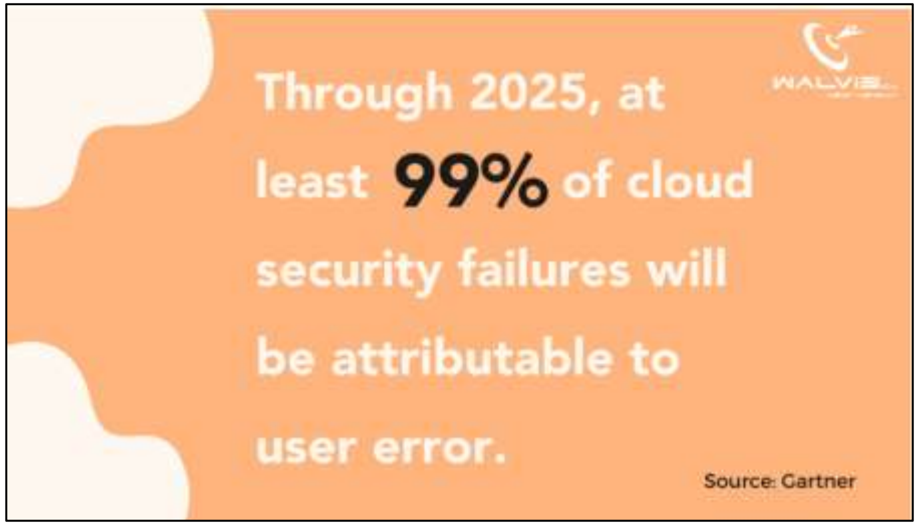


Fig 1: Variety of reasons for Cloud Misconfiguration

Source: https://www.helpnetsecurity.com/2018/10/05/cloud-misconfiguration/


Through 2025, at least **99%** of cloud security failures will be attributable to user error.

Source: Gartner

Fig 2: Gartner prediction on cloud security failures

Source: https://www.walvis.ca/blogs/How_Secure_Is_Cloud_Computing.php

Literature Review

Paper Title	Authors	Journal/Source	Major Insights	Research Gap
15 Top AWS RDS Misconfigurations to avoid in 2022	Cloudanix, 2022 [1]	https://blog.cloudanix.com/top-15-aws-rds-misconfigurations-2022	The article provides insights on top AWS RDS misconfigurations which can impact the data stored on DB	NA
Configuration Method of AWS Security Architecture That Is Applicable to the Cloud Lifecycle for Sustainable Social Network	Park, Se Joon Lee, Yong Joon Park, Won Hyung, 2022 [2]	Security and Communication Networks, volume 2022, Article id: 3686423	This research paper explains the cloud computing threats, a few top cloud attacks case scenarios, and a few basic security reference models to leverage	NA
AWS Security Reference Architecture	AWS, 2022 [3]	https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/security-reference-architecture.pdf	AWS explains all the security services it provides on its cloud platform and how utilizing them can increase the security posture of the architectures.	NA
Introduction to AWS Security	AWS, 2022 [4]	https://docs.aws.amazon.com/pdfs/whitepapers/latest/introduction-aws-security/introduction-aws-security.pdf	AWS explains about the shared responsibility model and how AWS works on priority to keep its infrastructure security components secured and updated.	AWS explains how it is the user's responsibility to configure their architectures to maximum security using its components.
How to Secure Your Website with AWS	AWS PS, 2021 [5]	https://www.aws.ps/how-to-secure-your-website-with-aws	The reference gives an overview of an architecture on AWS.	The reference doesn't mention any additional secured services to utilize with architecture.
Top 12 cloud security threats according to Cloud Security Alliance	Sheraz Malik, 2021 [6]	https://bitbytes.io/cloud-security-threats	The author explains the top 12 cloud security threats as per CSA.	This is just an overview of threat details and can consist of multiple components.

Literature Review Contd.

Paper Title	Authors	Journal/Source	Major Insights	Research Gap
Top 10 AWS Security Misconfiguration	Trend Micro, 2021 [7]	https://www.trendmicro.com/en_us/devops/21/k/top-10-aws-security-misconfigurations.html	Trend Micro provides insights on the top 10 AWS misconfigurations which can impact the architecture.	The article covers the most common AWS services which can be misconfigured but don't talk about the adequate controls to protect.
What Makes AWS Buckets Vulnerable to Ransomware and How to Mitigate the Threat	Ojasvi Nath, 2021 [8]	https://www.spiceworks.com/it-security/cyber-risk-management/news/aws-vulnerable-to-ransomware-attacks	The author provides statistics and insights on most common AWS S3 bucket misconfiguration	The article provides information on S3 related protection through policies but still requires further controls to protect buckets
4 Most Common Misconfigurations in AWS EC2 Instances	Akash Mahajan, 2021 [9]	https://kloudle.com/blog/4-most-common-misconfigurations-in-aws-ec2-instances	The author explains the common EC2 instances security issues	NA
51-Point AWS Security Configuration Checklist	McAfee, 2018 [10]	https://www.dlt.com/sites/default/files/resource-attachments/2019-09/Cloud-Cheat-Sheet-51-Point-AWS-Security-Configuration-Checklist_0_82.pdf	McAfee provides a checklist of a few AWS Security configuration checks which would be a huge benefit along with the integrated security controls	This explains mostly the policies and access restrictions and not on any additional secured components.
Data Security in Cloud Storage	Zhang, Yuan Xu, Chunxiang Shen, Xuemin Sherman, 2016, [11]	IJRITCC	The authors provide insights on huge amount of data being stored on cloud and the benefits of cloud computing handling the scalability and security of data.	The paper doesn't specifically mention any additional controls on data protection.

Problem Statement

- Companies roll out new workloads continuously on multiple AWS services without understanding the integrated security options or configuration of those services.
- Many Organizations have been pushed to migrate quickly to the cloud during this pandemic. They lack adequate security services or controls for further protection from cyber attacks.
- Lack of awareness of cloud security baseline architecture for the applications is one of the top causes of migration issues.
- Multiple advanced third-party security solutions are being introduced frequently; it is required to analyze them before integrating them with AWS architecture.

Problem Statement Contd.

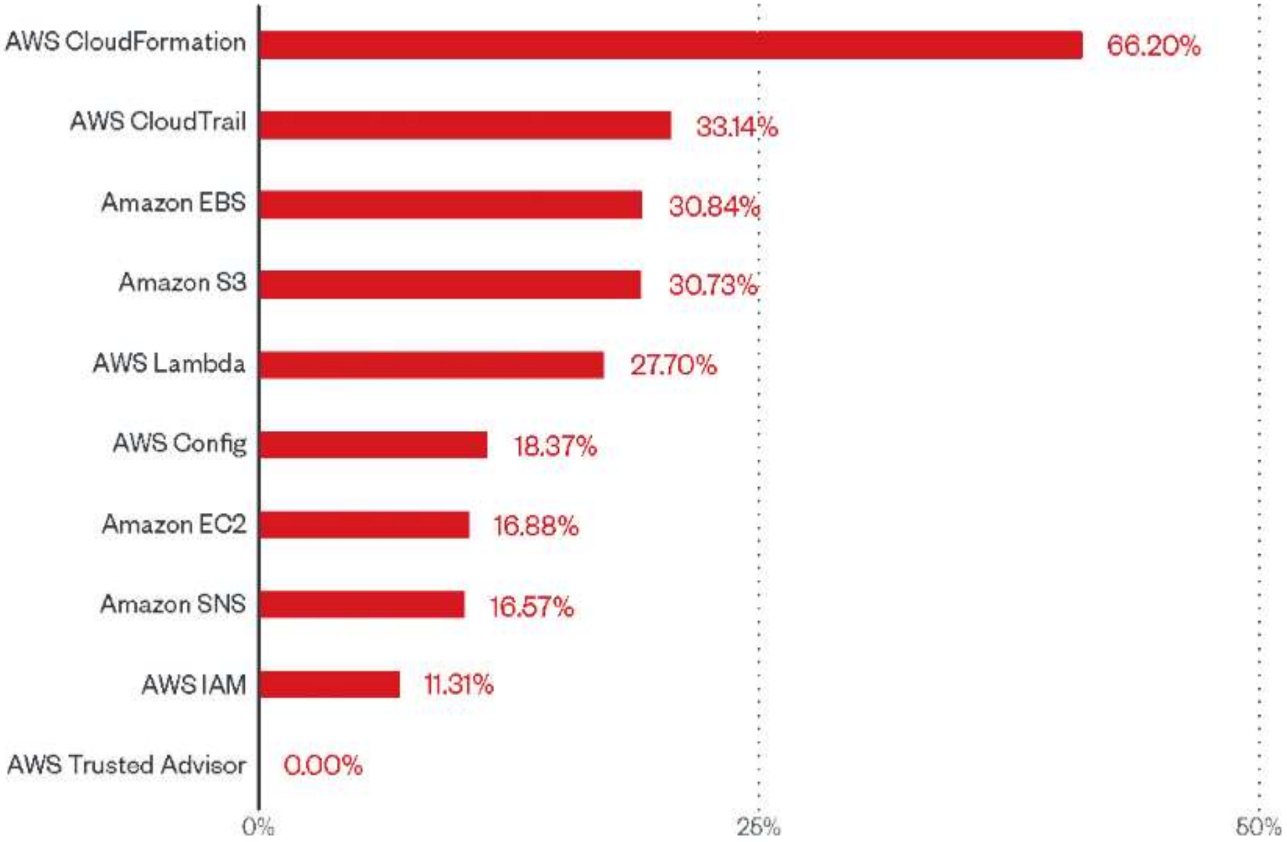


Fig 3. The misconfiguration rates of top 10 AWS services
Source: https://www.trendmicro.com/en_gb/devops/21/k/top-10-aws-security-misconfigurations.html

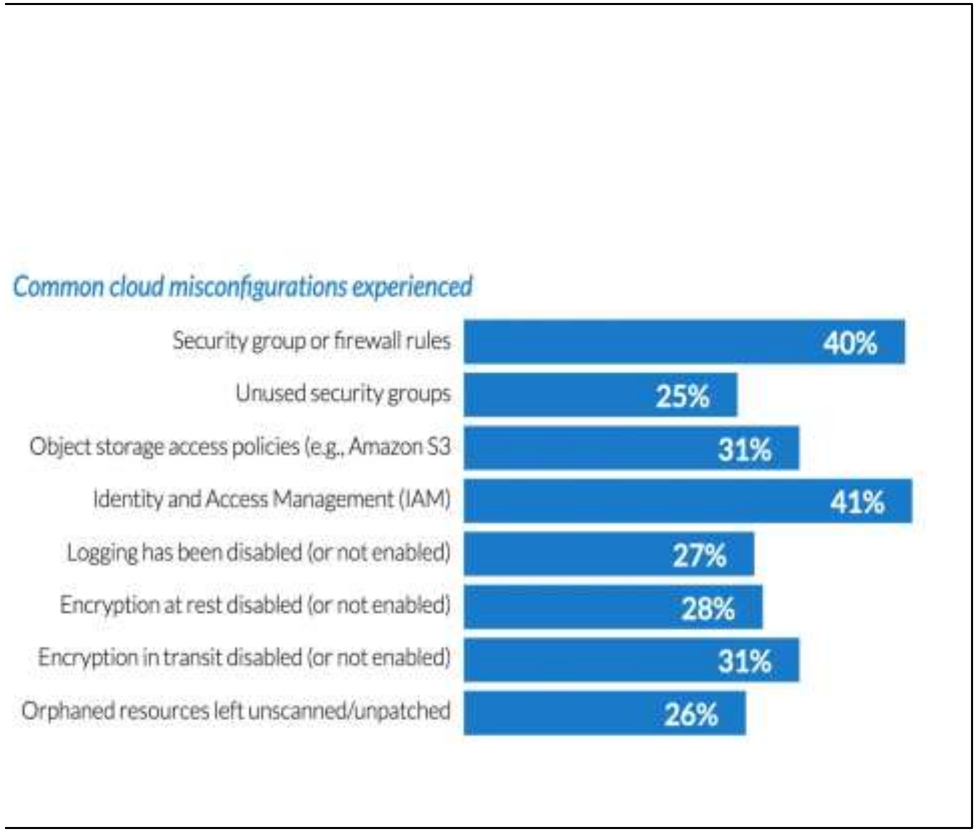
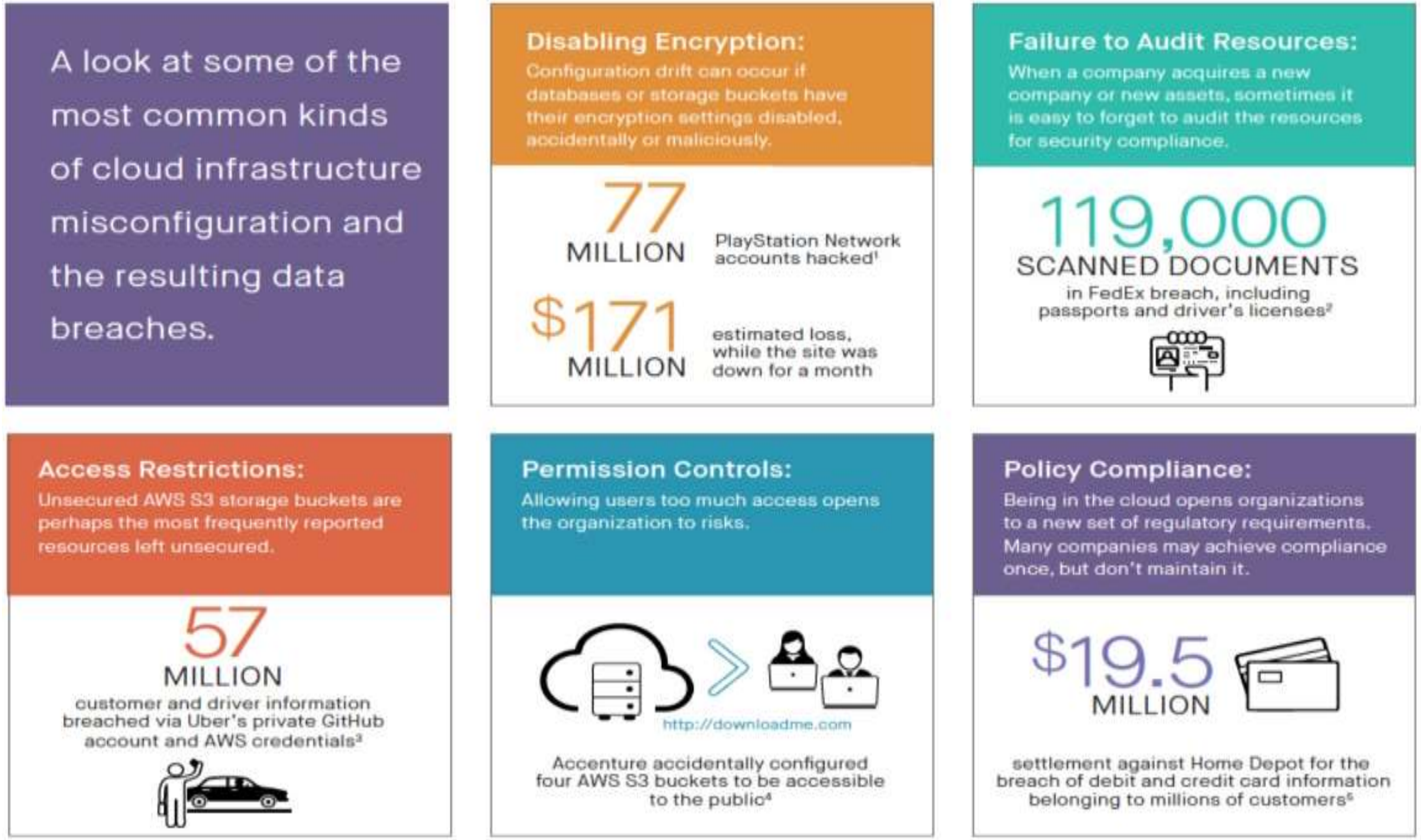


Fig 4: Common cloud misconfigurations
Source: https://www.infoworld.com/article/3653376/how-to-avoid-a-cloud-misconfiguration-attack.html

Problem Statement Contd.



A look at some of the most common kinds of cloud infrastructure misconfiguration and the resulting data breaches.

Disabling Encryption:
Configuration drift can occur if databases or storage buckets have their encryption settings disabled, accidentally or maliciously.

77 MILLION PlayStation Network accounts hacked[1]

$171 MILLION estimated loss, while the site was down for a month

Failure to Audit Resources:
When a company acquires a new company or new assets, sometimes it is easy to forget to audit the resources for security compliance.

119,000 SCANNED DOCUMENTS in FedEx breach, including passports and driver's licenses[2]

Access Restrictions:
Unsecured AWS S3 storage buckets are perhaps the most frequently reported resources left unsecured.

57 MILLION customer and driver information breached via Uber's private GitHub account and AWS credentials[3]

Permission Controls:
Allowing users too much access opens the organization to risks.

Accenture accidentally configured four AWS S3 buckets to be accessible to the public[4]

Policy Compliance:
Being in the cloud opens organizations to a new set of regulatory requirements. Many companies may achieve compliance once, but don't maintain it.

$19.5 MILLION settlement against Home Depot for the breach of debit and credit card information belonging to millions of customers[5]

Fig 5: Most common cloud misconfiguration and the data breaches

Source: https://www.fugue.co/blog/2018-09-11-cloud-infrastructure-misconfiguration-what-every-ciso-should-know-part-iii.html

Objectives

- Propose a secured cloud architectural design keeping the data secured at rest and in transit.
- Develop an integrated AWS-managed advanced security and monitoring services to have robust security even with multiple third-party services.
- Create a secured architecture baseline for organizations who would like to refer them to deploy or migrate their software solution to AWS quickly.
- Assist organizations in reviewing their current architecture on the cloud and introduce the proposed security components hence improving the security posture.

Architecture Design: Deployed on EC2

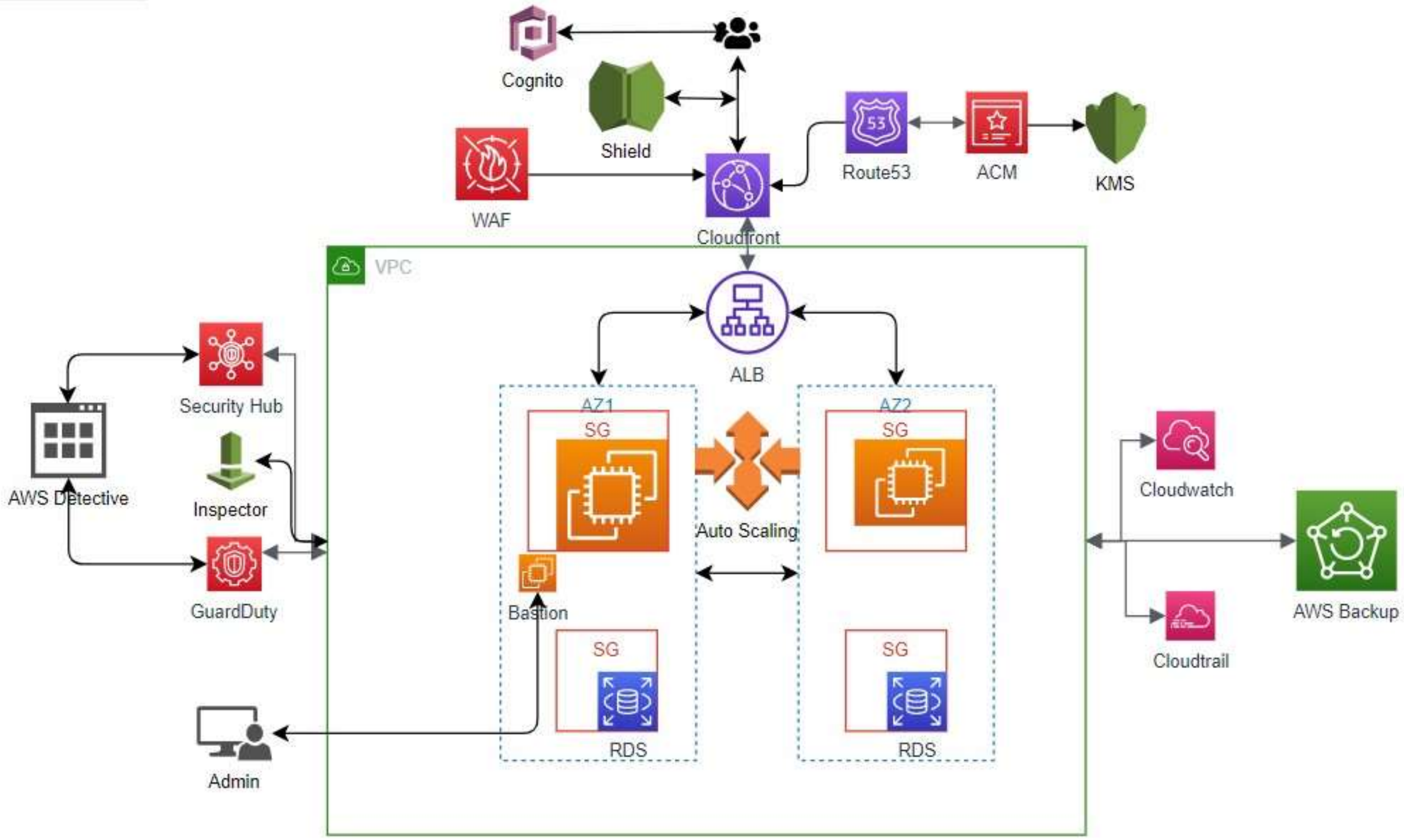


Fig 6: Web application architecture deployed on EC2

Architecture Design: Deployed on S3

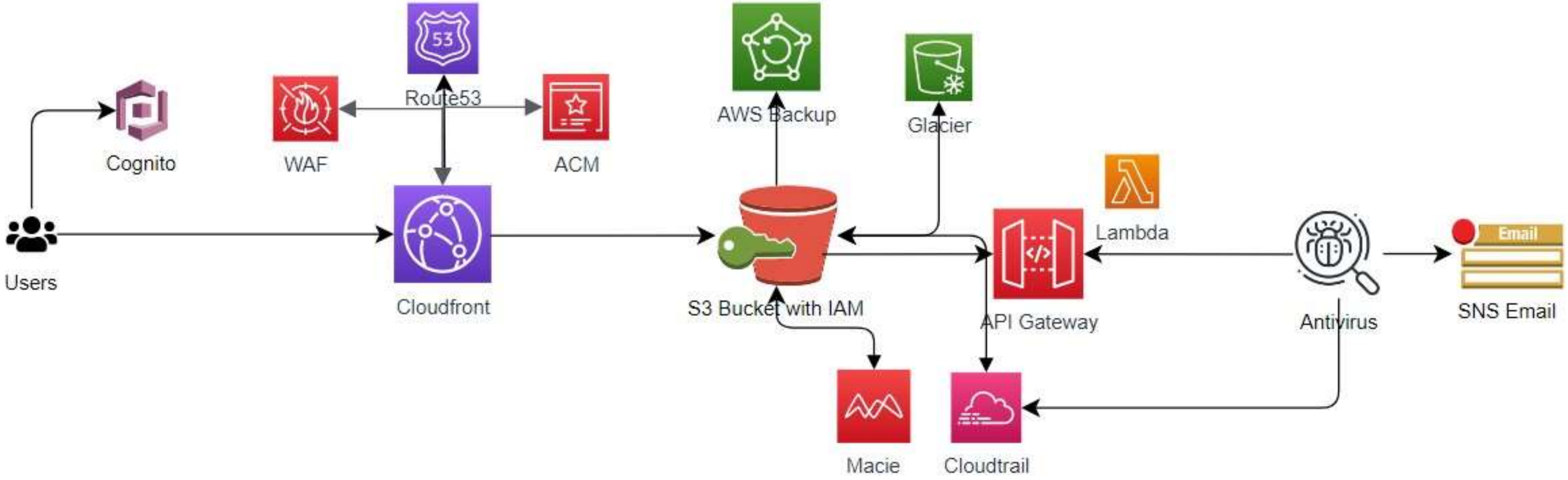


Fig 7: Application architecture deployed on S3

Implementation: Deployed on EC2

The web application framework is deployed on EC2 and configured to interact with RDS DB for storing web and user data.

The architecture is having auto-scaling feature during heavy load. The site is publicly accessible on TLS through CloudFront only with ALB as the backend and the EC2 instance endpoint is not accessible from the internet.

The website is protected from DDoS and web application attacks protected by WAF. The architecture is protected further by multiple AWS services and logging and monitoring enabled.

The web server interacts with RDS MySQL DB for storing web data and user data. The RDS DB is encrypted with a KMS key and the RDS endpoint is not open to the public internet.

For admin support on the EC2 web server and RDS DB, the admin can connect through the Bastion host or Client VPN.

Implementation: Deployed on S3

The web application code is deployed on an S3 bucket and configured for hosting the server.

Users can connect to the web server endpoint on TLS through CloudFront which has Origin Access Identity configured to the respective S3 bucket.

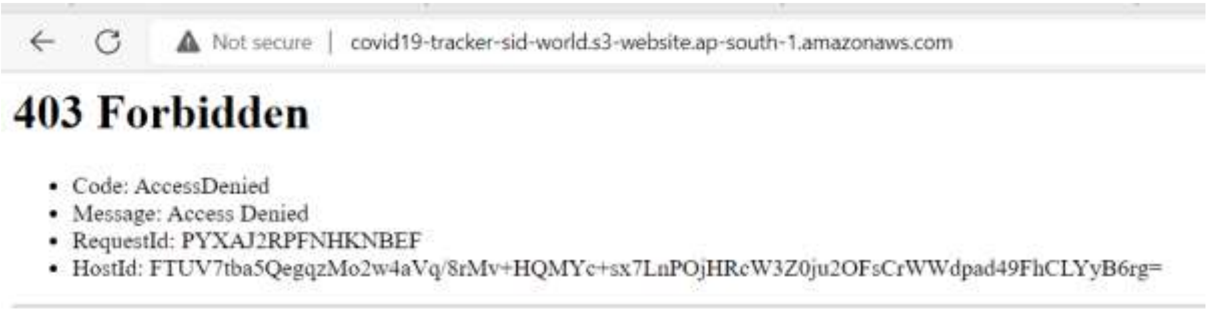
The CloudFront is protected by WAF and other security services are integrated with the architecture.

The S3 bucket is not accessible and is blocked from the internet.

The bucket is configured with an Antivirus solution so that every file uploaded to the bucket gets scanned. If a file is found infected then it gets deleted from the bucket and an email notification is triggered to the Admin.

The Macie services also monitor the bucket for any sensitive files or credentials files if uploaded and notify. Backup and cloud trail are also integrated

Testing and Validation

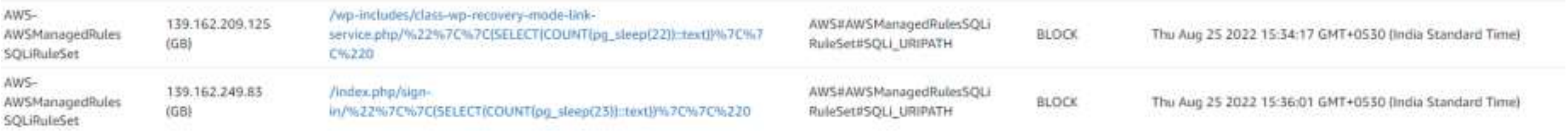


Not secure | covid19-tracker-sid-world.s3-website.ap-south-1.amazonaws.com

403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: PYXAJ2RPFNHKNBEF
- HostId: FTUV7tba5QegqzMo2w4aVq/8rMv+HQMYc+sx7LnPOjHRcW3Z0ju2OFsCrWWdpad49FhCLYyB6rg=

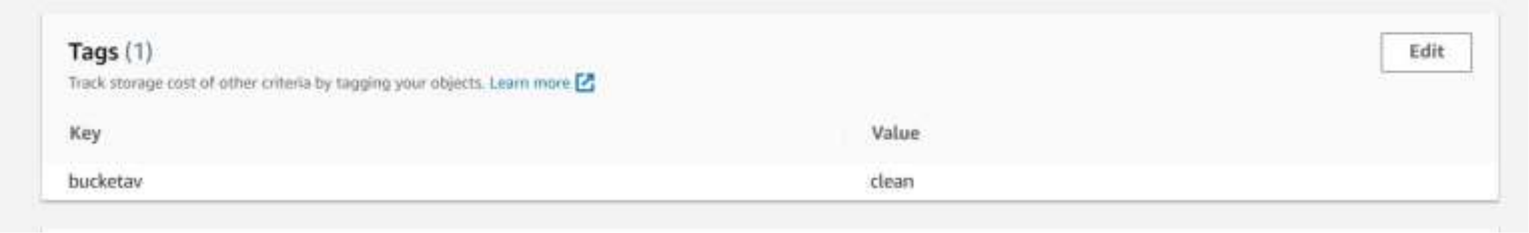
Fig 8: S3 endpoint not accessible directly on the internet



AWS-AWSManagedRulesSQLiRuleSet	139.162.209.125 (GB)	/wp-includes/class-wp-recovery-mode-link-service.php/%22%7C%7C(SELECT(COUNT(pg_sleep(22))::text))%7C%7C%220	AWS#AWSManagedRulesSQLiRuleSet#SQLi_URIPATH	BLOCK	Thu Aug 25 2022 15:34:17 GMT+0530 (India Standard Time)
AWS-AWSManagedRulesSQLiRuleSet	139.162.249.83 (GB)	/index.php/sign-in/%22%7C%7C(SELECT(COUNT(pg_sleep(23))::text))%7C%7C%220	AWS#AWSManagedRulesSQLiRuleSet#SQLi_URIPATH	BLOCK	Thu Aug 25 2022 15:36:01 GMT+0530 (India Standard Time)

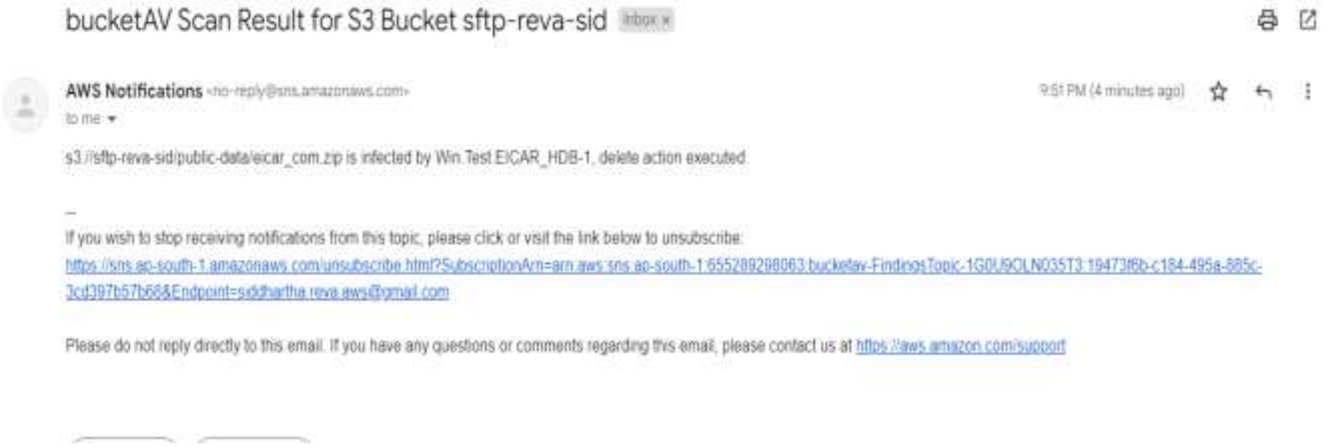
Fig 9: SQL Injection attacks blocked by WAF

Testing and Validation


Tags (1)
Track storage cost of other criteria by tagging your objects. Learn more

Key	Value
bucketav	clean

Fig 10: AntiVirus scan status for each object uploaded on S3 bucket


bucketAV Scan Result for S3 Bucket sftp-reva-sid

AWS Notifications <no-reply@sns.amazonaws.com>
to me

9:51 PM (4 minutes ago)

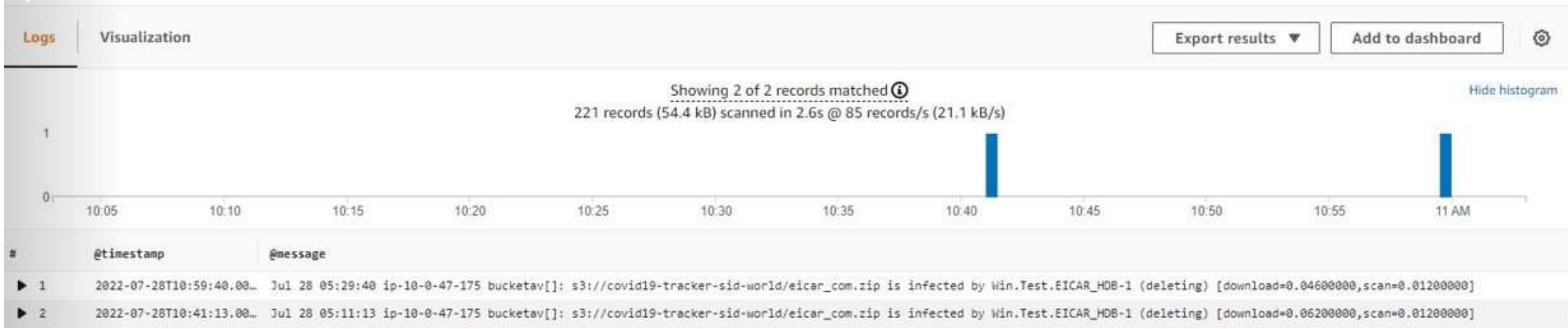
s3://sftp-reva-sid/public-data/eicar_com.zip is infected by Win.Test.EICAR_HDB-1, delete action executed.

--
If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
https://sns.ap-south-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:ap-south-1:655289298063:bucketav-FindingsTopic-1G0U9OLN035T3:19473f6b-c184-495a-885c-3cd397b57b68&Endpoint=siddhartha.reva.aws@gmail.com

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at https://aws.amazon.com/support

Fig 11: SNS email notification sent when infected object detected

Testing and Validation

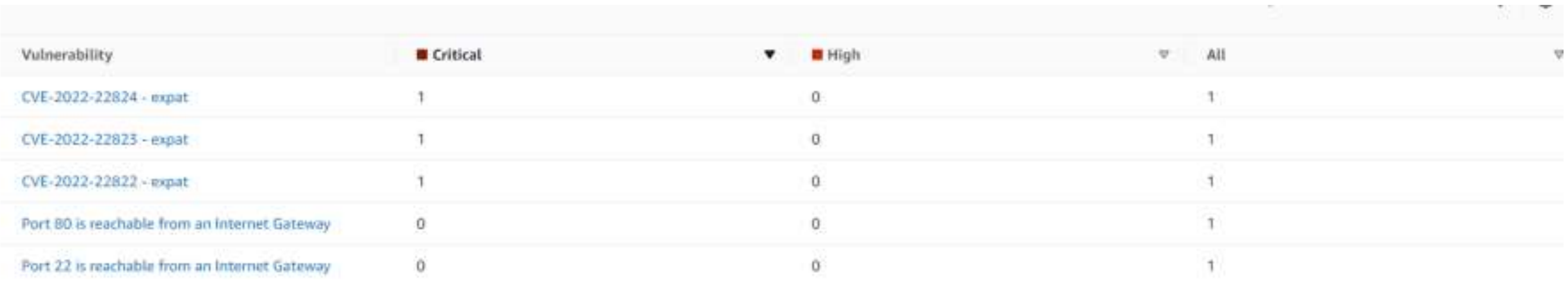


Showing 2 of 2 records matched

221 records (54.4 kB) scanned in 2.6s @ 85 records/s (21.1 kB/s)

```
#      @timestamp                 @message
▶ 1    2022-07-28T10:59:40.00…    Jul 28 05:29:40 ip-10-0-47-175 bucketav[]: s3://covid19-tracker-sid-world/eicar_com.zip is infected by Win.Test.EICAR_HDB-1 (deleting) [download=0.04600000,scan=0.01200000]
▶ 2    2022-07-28T10:41:13.00…    Jul 28 05:11:13 ip-10-0-47-175 bucketav[]: s3://covid19-tracker-sid-world/eicar_com.zip is infected by Win.Test.EICAR_HDB-1 (deleting) [download=0.06200000,scan=0.01200000]
```

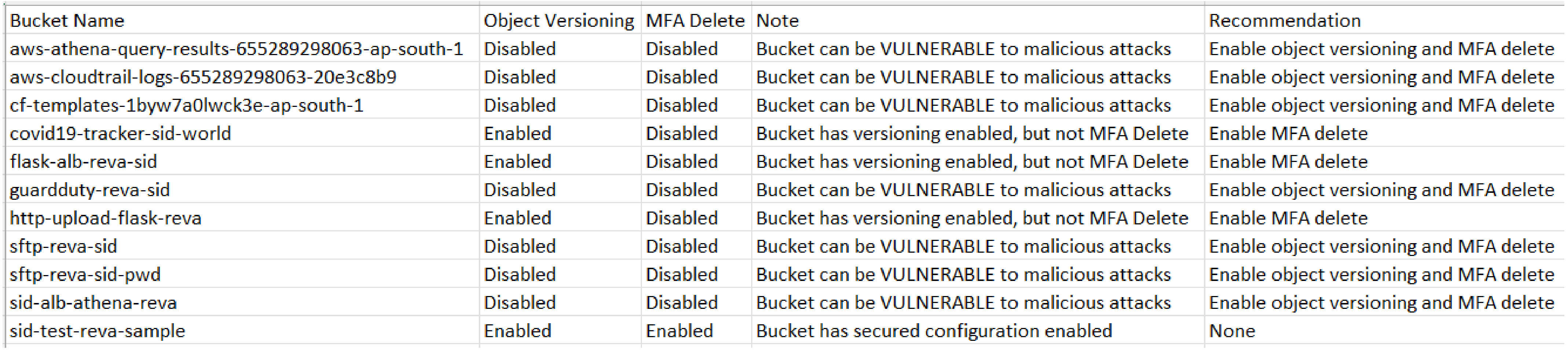
Fig 12: Cloudwatch logs capturing infected file



Vulnerability	🟥 Critical ▼	🟥 High	All
CVE-2022-22824 - expat	1	0	1
CVE-2022-22823 - expat	1	0	1
CVE-2022-22822 - expat	1	0	1
Port 80 is reachable from an Internet Gateway	0	0	1
Port 22 is reachable from an Internet Gateway	0	0	1

Fig 13: AWS Inspector vulnerability scanning

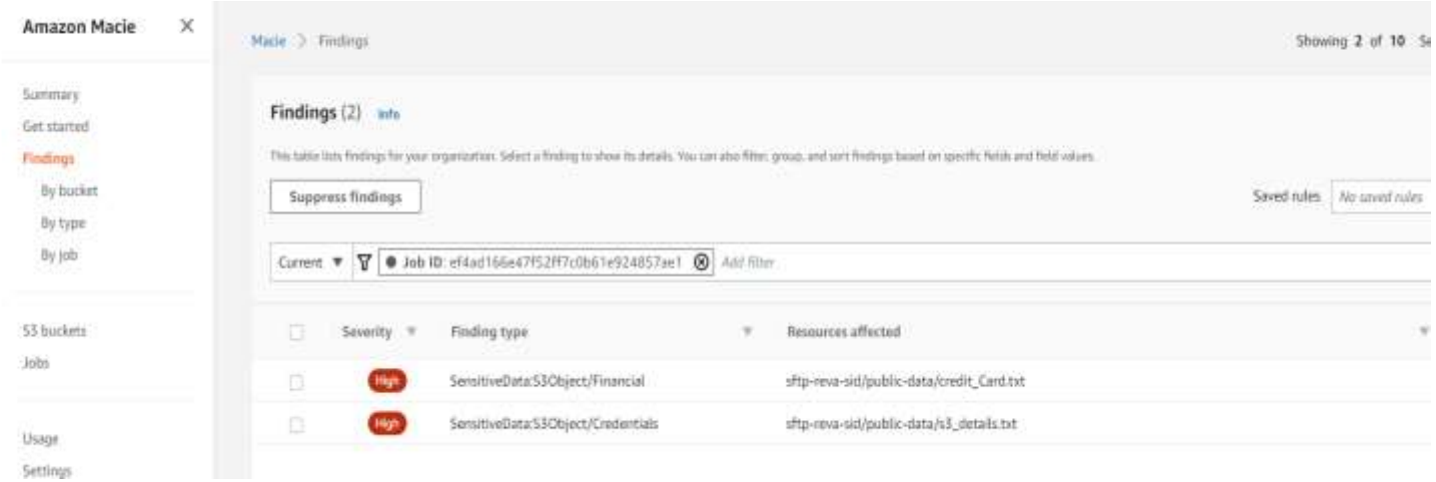
Testing and Validation



Bucket Name	Object Versioning	MFA Delete	Note	Recommendation
aws-athena-query-results-655289298063-ap-south-1	Disabled	Disabled	Bucket can be VULNERABLE to malicious attacks	Enable object versioning and MFA delete
aws-cloudtrail-logs-655289298063-20e3c8b9	Disabled	Disabled	Bucket can be VULNERABLE to malicious attacks	Enable object versioning and MFA delete
cf-templates-1byw7a0lwck3e-ap-south-1	Disabled	Disabled	Bucket can be VULNERABLE to malicious attacks	Enable object versioning and MFA delete
covid19-tracker-sid-world	Enabled	Disabled	Bucket has versioning enabled, but not MFA Delete	Enable MFA delete
flask-alb-reva-sid	Enabled	Disabled	Bucket has versioning enabled, but not MFA Delete	Enable MFA delete
guardduty-reva-sid	Disabled	Disabled	Bucket can be VULNERABLE to malicious attacks	Enable object versioning and MFA delete
http-upload-flask-reva	Enabled	Disabled	Bucket has versioning enabled, but not MFA Delete	Enable MFA delete
sftp-reva-sid	Disabled	Disabled	Bucket can be VULNERABLE to malicious attacks	Enable object versioning and MFA delete
sftp-reva-sid-pwd	Disabled	Disabled	Bucket can be VULNERABLE to malicious attacks	Enable object versioning and MFA delete
sid-alb-athena-reva	Disabled	Disabled	Bucket can be VULNERABLE to malicious attacks	Enable object versioning and MFA delete
sid-test-reva-sample	Enabled	Enabled	Bucket has secured configuration enabled	None

Fig 14: Automation script enabled on buckets to send details on each bucket security configuration

Testing and Validation



Amazon Macie ✕

- Summary
- Get started
- Findings
  - By bucket
  - By type
  - By job
- S3 buckets
- Jobs
- Usage
- Settings

Macie > Findings

Showing 2 of 10

Findings (2) Info

This table lists findings for your organization. Select a finding to show its details. You can also filter, group, and sort findings based on specific fields and field values.

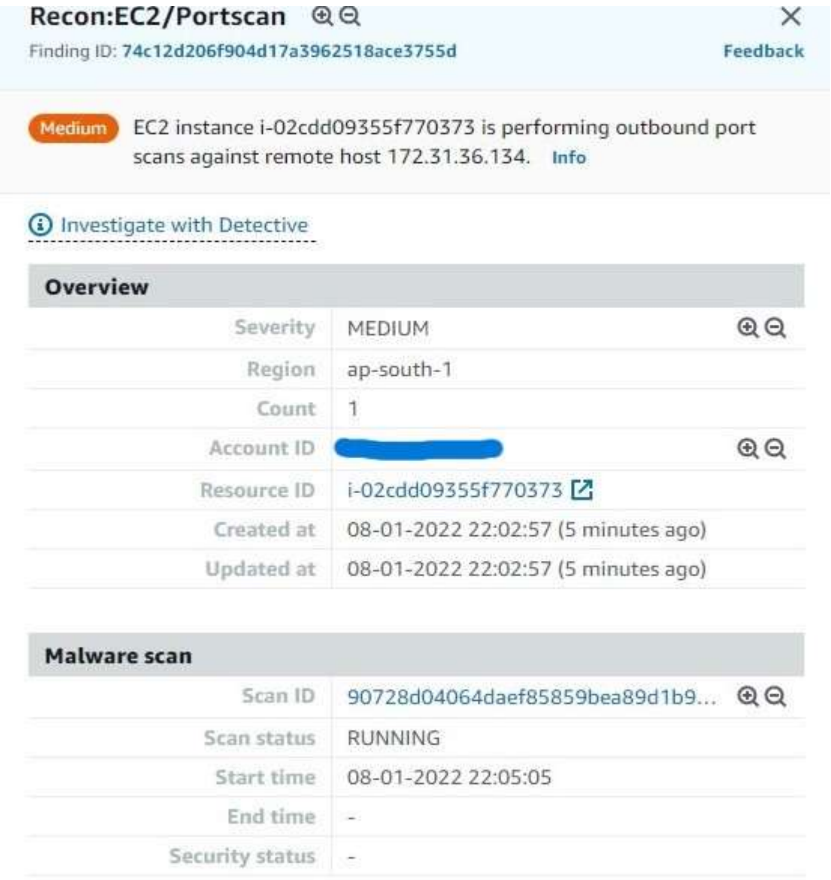
Suppress findings

Saved rules: No saved rules

Current ▼ | Job ID: ef4ad166e47f52ff7c0b61e924857ae1 ⊗ | Add filter

□	Severity	Finding type	Resources affected
□	High	SensitiveData:S3Object/Financial	sftp-reva-sid/public-data/credit_Card.txt
□	High	SensitiveData:S3Object/Credentials	sftp-reva-sid/public-data/s3_details.txt

Fig 15: AWS Macie detecting sensitive files as DLP mechanism



Recon:EC2/Portscan ✕

Finding ID: 74c12d206f904d17a3962518ace3755d Feedback

Medium EC2 instance i-02cdd09355f770373 is performing outbound port scans against remote host 172.31.36.134. Info

Investigate with Detective

Overview

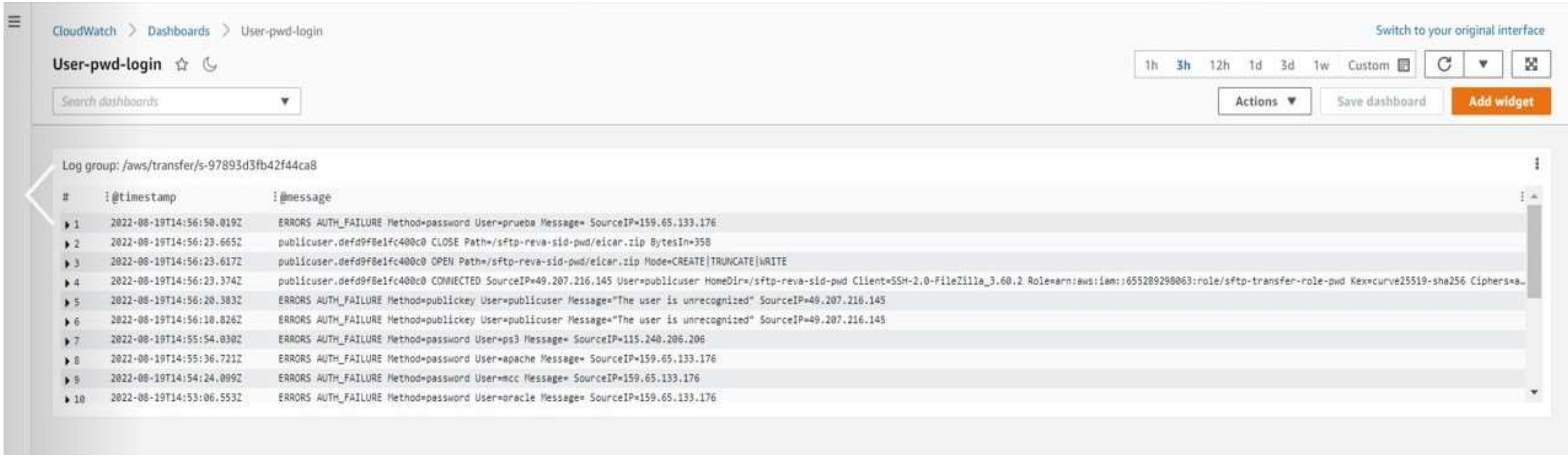
Severity	MEDIUM
Region	ap-south-1
Count	1
Account ID	[redacted]
Resource ID	i-02cdd09355f770373
Created at	08-01-2022 22:02:57 (5 minutes ago)
Updated at	08-01-2022 22:02:57 (5 minutes ago)

Malware scan

Scan ID	90728d04064daef85859bea89d1b9...
Scan status	RUNNING
Start time	08-01-2022 22:05:05
End time	-
Security status	-

Fig 16: Guard duty detecting a port scan attempt

Testing and Validation

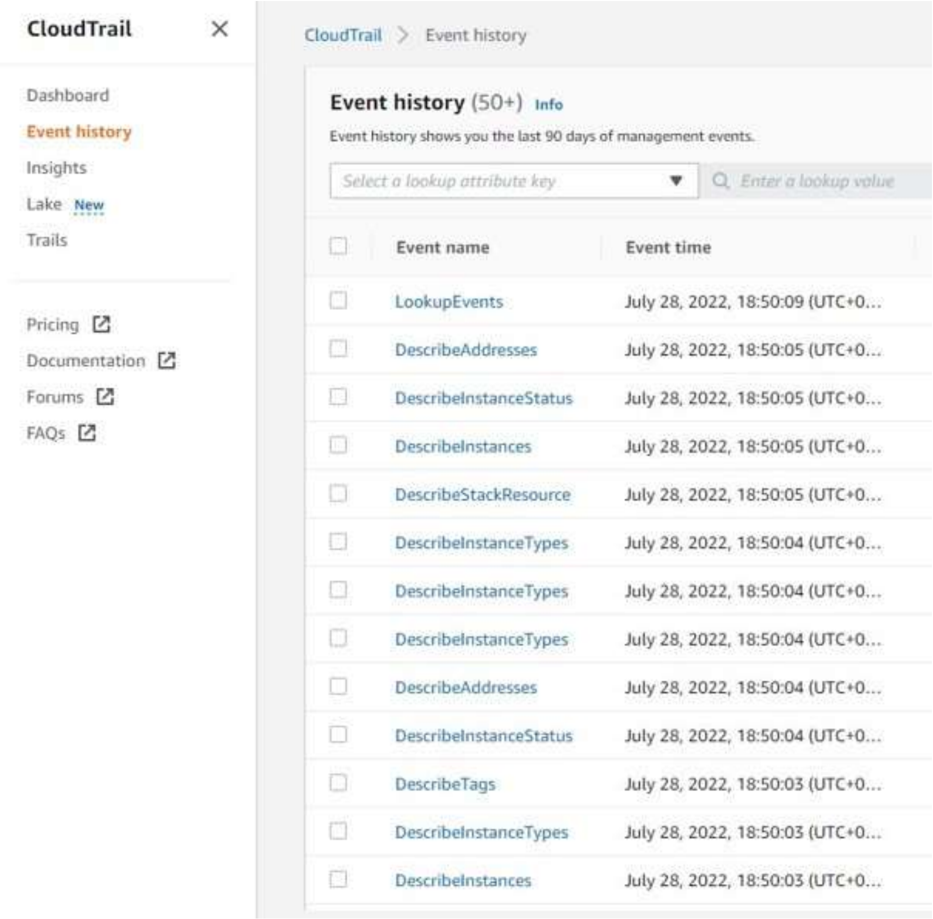

CloudWatch > Dashboards > User-pwd-login
Switch to your original interface
User-pwd-login
Search dashboards
1h 3h 12h 1d 3d 1w Custom
Actions
Save dashboard
Add widget

```
Log group: /aws/transfer/s-97893d3fb42f44ca8

#     @timestamp                  @message
▸ 1   2022-08-19T14:56:50.019Z    ERRORS AUTH_FAILURE Method=password User=prueba Message= SourceIP=159.65.133.176
▸ 2   2022-08-19T14:56:23.665Z    publicuser.defd9f8e1fc400c0 CLOSE Path=/sftp-reva-sid-pwd/eicar.zip BytesIn=358
▸ 3   2022-08-19T14:56:23.617Z    publicuser.defd9f8e1fc400c0 OPEN Path=/sftp-reva-sid-pwd/eicar.zip Mode=CREATE|TRUNCATE|WRITE
▸ 4   2022-08-19T14:56:23.374Z    publicuser.defd9f8e1fc400c0 CONNECTED SourceIP=49.207.216.145 User=publicuser HomeDir=/sftp-reva-sid-pwd Client=SSH-2.0-FileZilla_3.60.2 Role=arn:aws:iam::655289298063:role/sftp-transfer-role-pwd Kex=curve25519-sha256 Ciphers=a…
▸ 5   2022-08-19T14:56:20.383Z    ERRORS AUTH_FAILURE Method=publickey User=publicuser Message="The user is unrecognized" SourceIP=49.207.216.145
▸ 6   2022-08-19T14:56:18.826Z    ERRORS AUTH_FAILURE Method=publickey User=publicuser Message="The user is unrecognized" SourceIP=49.207.216.145
▸ 7   2022-08-19T14:55:54.030Z    ERRORS AUTH_FAILURE Method=password User=ps3 Message= SourceIP=115.240.206.206
▸ 8   2022-08-19T14:55:36.721Z    ERRORS AUTH_FAILURE Method=password User=apache Message= SourceIP=159.65.133.176
▸ 9   2022-08-19T14:54:24.099Z    ERRORS AUTH_FAILURE Method=password User=mcc Message= SourceIP=159.65.133.176
▸ 10  2022-08-19T14:53:06.553Z    ERRORS AUTH_FAILURE Method=password User=oracle Message= SourceIP=159.65.133.176
```

Fig 17: Brute force password attempt detected and blocked

Testing and Validation



Event history (50+) Info

Event history shows you the last 90 days of management events.

Select a lookup attribute key ▼ Enter a lookup value

□	Event name	Event time
□	LookupEvents	July 28, 2022, 18:50:09 (UTC+0...
□	DescribeAddresses	July 28, 2022, 18:50:05 (UTC+0...
□	DescribeInstanceStatus	July 28, 2022, 18:50:05 (UTC+0...
□	DescribeInstances	July 28, 2022, 18:50:05 (UTC+0...
□	DescribeStackResource	July 28, 2022, 18:50:05 (UTC+0...
□	DescribeInstanceTypes	July 28, 2022, 18:50:04 (UTC+0...
□	DescribeInstanceTypes	July 28, 2022, 18:50:04 (UTC+0...
□	DescribeInstanceTypes	July 28, 2022, 18:50:04 (UTC+0...
□	DescribeAddresses	July 28, 2022, 18:50:04 (UTC+0...
□	DescribeInstanceStatus	July 28, 2022, 18:50:04 (UTC+0...
□	DescribeTags	July 28, 2022, 18:50:03 (UTC+0...
□	DescribeInstanceTypes	July 28, 2022, 18:50:03 (UTC+0...
□	DescribeInstances	July 28, 2022, 18:50:03 (UTC+0...

Fig 18: CloudTrail logs for audit purposes

Analysis and Results

This paper has demonstrated on two common secured application architectures deployed on EC2 and S3 without exposing the S3, EC2 and RDS endpoints to the internet while protecting them from cyber attacks.

Multiple AWS-offered security services were also integrated, successfully.

AWS takes care of keeping them updated removing the burden on organization admins.

The solutions provide a baseline architecture idea to organizations that would like to migrate to the cloud for their product and operations and remain secured on AWS.

Through the solution, we have demonstrated how the architectures can remain secure when multiple cyber attack attempts are tested on them while checking each component functionality.

The whole solution is on the AWS cloud and utilizes AWS-offered security and monitoring services without relying on third-party solutions. This is encouraging to organizations planning migration.

Conclusion and Future Scope

❖ This paper demonstrated a couple of common applications integrated with a few AWS-provided advanced security services as some third-party services are very advanced and can be sometimes complex and expensive when integrated with AWS.

❖ The architectures can be further advanced to accept MFA using any identity provider like OKTA, or OneLogin which will enhance the authentication security. Multiple third-party IDS, IPS, and Firewalls can also be integrated to provide defense in depth.

❖ There are a few new AWS solutions like AWS Security Hub, AWS advanced network firewall, and AWS Audit which can be integrated with the architectures for a strong cloud security posture management.

❖ Multiple automation scripts or jobs can be developed for further assistance in strengthening security. Logs generated from various AWS services can be analyzed on compatible monitoring tools like Splunk, and Kibana for enhanced monitoring and alerting mechanisms.

References

[1] K. Ghule, “The 15 Common AWS RDS Misconfigurations,” 2022. https://blog.cloudanix.com/top-15-aws-rds-misconfigurations-2022/

[2] Se-Joon Park, Yong-Joon Lee, Won-Hyung Park “Configuration Method of AWS Security Architecture That Is Applicable to the Cloud Lifecycle for Sustainable Social Network,” 2022. https://www.hindawi.com/journals/scn/2022/3686423/ [2]

[3] AWS “AWS Security Reference Architecture,” 2022. https://docs.aws.amazon.com/pdfs/prescriptive-guidance/latest/security-reference-architecture/security-reference-architecture.pdf

[4] AWS “Introduction to AWS Security,” 2022. https://docs.aws.amazon.com/pdfs/whitepapers/latest/introduction-aws-security/introduction-aws-security.pdf

[5] AWS PS “How to Secure Your Website with AWS,” 2021. https://www.aws.ps/how-to-secure-your-website-with-aws

[6] S. Malik “Top 12 cloud security threats according to Cloud Security Alliance,” 2021. https://bitbytes.io/cloud-security-threats

[7] Trend Micro “Top 10 AWS Security Misconfiguration,” 2021. https://www.trendmicro.com/en_us/devops/21/k/top-10-aws-security-misconfigurations.html

[8] O. Nath “What Makes AWS Buckets Vulnerable to Ransomware and How to Mitigate the Threat,” 2021. https://www.spiceworks.com/it-security/cyber-risk-management/news/aws-vulnerable-to-ransomware-attacks

[9] A. Mahajan “4 Most Common Misconfigurations in AWS EC2 Instances,” 2021. https://kloudle.com/blog/4-most-common-misconfigurations-in-aws-ec2-instances

[10] McAfee “51-Point AWS Security Configuration Checklist,” 2018. https://www.dlt.com/sites/default/files/resource-attachments/2019-09/Cloud-Cheat-Sheet-51-Point-AWS-Security-Configuration-Checklist_0_82.pdf

[11] Zhang, Y., Xu, C., & Shen, X. S. (2020). Data Security in Cloud Storage. Springer Singapore, March, 310–313.

THANK YOU