

S3 File Upload and Integrity Validation Using SHA-256 Checksum

Contents

1. Objective :	2
2. Checksum	2
Checksum = the proof that the file was not changed.	2
It verifies:	2
2.1 HOW checksum integrity check works (concept)	2
Step A — Calculate checksum on your local file	2
Step B — Get checksum from S3	2
3. Configure AWS using credentials via cli.	3
4. Create a new test file	3
5. Compute local checksum (original file)	4
6. Upload the file to AWS S3	4
7. Download the same file back	4
8. Compute the Checksum of download file	4
9. Compare both checksums	5
10. Conclusion	6

Complete step-by-step documentation

1. Objective :

- Upload a file from a local machine to an Amazon S3 bucket
- Validate the **data integrity** of the uploaded file
- Understand **checksum (SHA-256)** and how it is used to detect corruption
- Confirm that the file uploaded to S3 matches the original file exactly

This is a critical cloud engineering skill used in backups, migrations, and secure data transfer.

2. Checksum

Checksum = the proof that the file was not changed.

It verifies:

- No corruption
- No modification
- No partial upload
- No network error
- No tampering

2.1 HOW checksum integrity check works (concept)

Step A — Calculate checksum on your local file

You run:

```
CertUtil -hashfile myfile.txt SHA256
```

Local checksum might be:

AAA111BBB222CCC333...

Step B — Get checksum from S3

Two ways:

1. If S3 stores checksum metadata

(using head-object):

```
ChecksumSHA256 = "AAA111BBB222CCC333..."
```

If the checksums match → integrity = OK.

2. If S3 does NOT store checksum (like your case)

Then do this:

Download the file:

```
aws s3 cp s3://bucket/myfile.txt downloaded.txt
```

Calculate checksum of downloaded file:

```
CertUtil -hashfile downloaded.txt SHA256
```

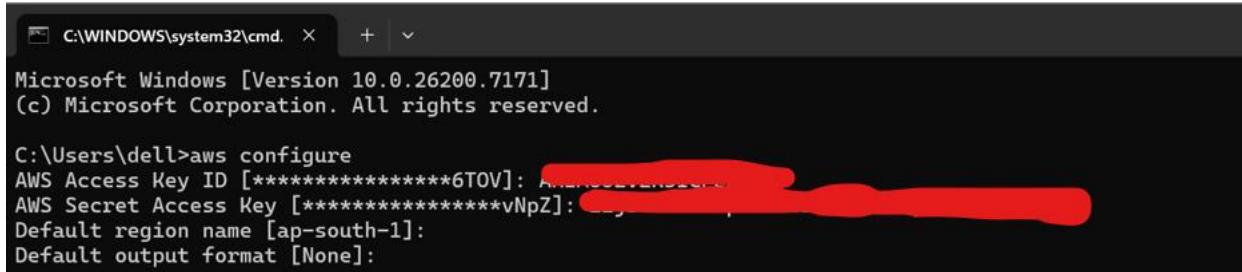
Compare:

Local: AAA111BBB222CCC333

Downloaded: AAA111BBB222CCC333

If they match → file is exactly identical.

3. Configure AWS using credentials via cli.



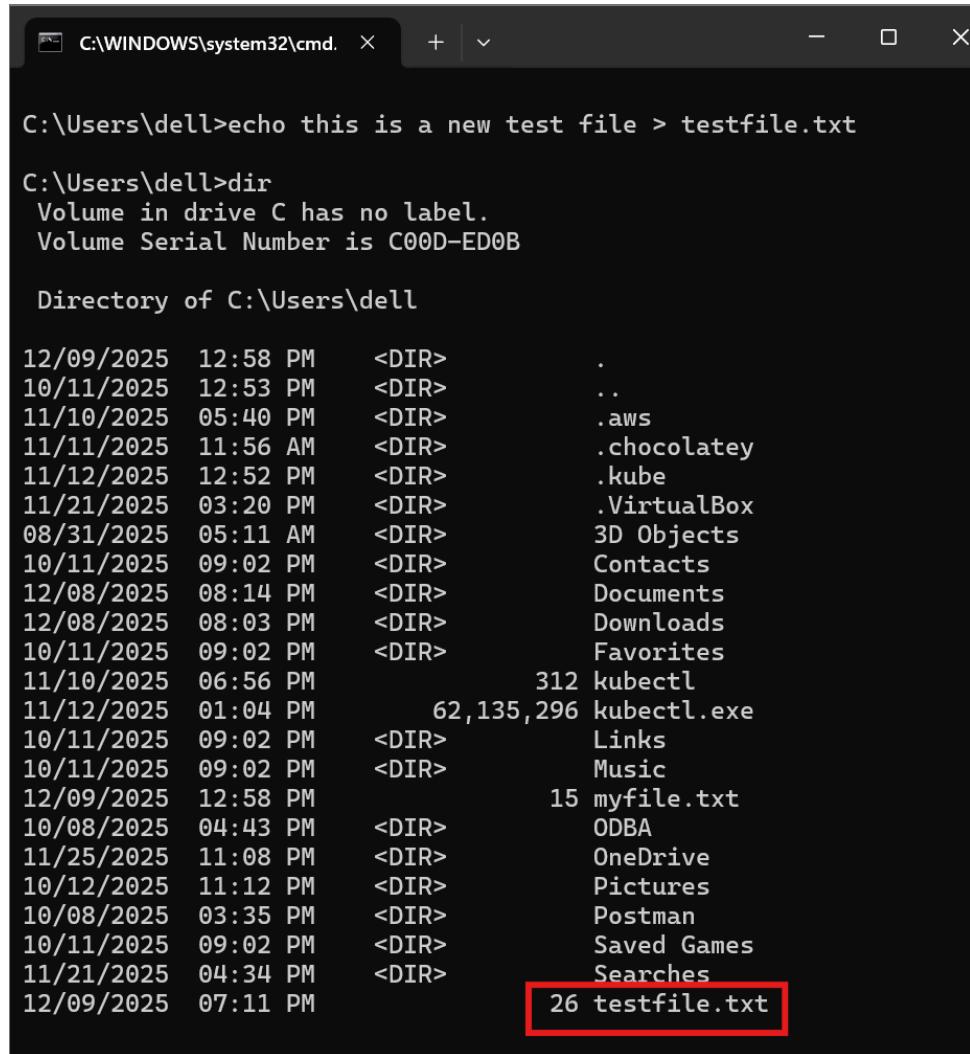
```
C:\WINDOWS\system32\cmd. × + ▾
Microsoft Windows [Version 10.0.26200.7171]
(c) Microsoft Corporation. All rights reserved.

C:\Users\dell>aws configure
AWS Access Key ID [*****6TOV]: XXXXXXXXXX
AWS Secret Access Key [*****vNpZ]: XXXXXXXXXX
Default region name [ap-south-1]:
Default output format [None]:
```

4. Create a new test file

run this command: echo this is a new test file > testfile.txt

verify it exists: >>> dir testfile.txt



```
C:\WINDOWS\system32\cmd. × + ▾
C:\Users\dell>echo this is a new test file > testfile.txt

C:\Users\dell>dir
Volume in drive C has no label.
Volume Serial Number is C00D-ED0B

Directory of C:\Users\dell

12/09/2025  12:58 PM    <DIR>        .
10/11/2025  12:53 PM    <DIR>        ..
11/10/2025  05:40 PM    <DIR>        .aws
11/11/2025  11:56 AM    <DIR>        .chocolatey
11/12/2025  12:52 PM    <DIR>        .kube
11/21/2025  03:20 PM    <DIR>        .VirtualBox
08/31/2025  05:11 AM    <DIR>        3D Objects
10/11/2025  09:02 PM    <DIR>        Contacts
12/08/2025  08:14 PM    <DIR>        Documents
12/08/2025  08:03 PM    <DIR>        Downloads
10/11/2025  09:02 PM    <DIR>        Favorites
11/10/2025  06:56 PM    312 kubectl
11/12/2025  01:04 PM    62,135,296 kubectl.exe
10/11/2025  09:02 PM    <DIR>        Links
10/11/2025  09:02 PM    <DIR>        Music
12/09/2025  12:58 PM    15 myfile.txt
10/08/2025  04:43 PM    <DIR>        ODBA
11/25/2025  11:08 PM    <DIR>        OneDrive
10/12/2025  11:12 PM    <DIR>        Pictures
10/08/2025  03:35 PM    <DIR>        Postman
10/11/2025  09:02 PM    <DIR>        Saved Games
11/21/2025  04:34 PM    <DIR>        Searches
12/09/2025  07:11 PM    26 testfile.txt
```

5. Compute local checksum (original file)

Run : CertUtil -hashfile testfile.txt SHA256

```
C:\Users\dell>CertUtil -hashfile testfile.txt SHA256
SHA256 hash of testfile.txt:
898393ccb6f176cc783e9417ad1af2453e7f9972ba64330c17166f6c0f655c8d
CertUtil: -hashfile command completed successfully.
```

This is the **digital fingerprint** of your file.

6. Upload the file to AWS S3

Run : aws s3 cp testfile.txt s3://preeti-demo-bucket-2025-12-09/

```
C:\Windows\system32\cmd. X + v - X
CertUtil: -hashfile command completed successfully.

C:\Users\dell>aws s3 cp testfile.txt s3://preeti-demo-bucket-2025-12-09/
Completed 26 Bytes/26 Bytes (38 Bytes/s) with 1 file(s) remaininupload: ./testfile.txt to s3://preeti-demo-bucket-2025-12-09/testfile.txt

C:\Users\dell>
```

you should see:

```
upload: ./testfile.txt to s3://preeti-demo-bucket-2025-12-09/testfile.txt
```

This means the upload succeeded.

7. Download the same file back

Run : aws s3 cp s3://preeti-demo-bucket-2025-12-09/testfile.txt downloaded.txt

```
C:\Users\dell>
C:\Users\dell>aws s3 cp s3://preeti-demo-bucket-2025-12-09/testfile.txt downloaded.txt
Completed 26 Bytes/26 Bytes (41 Bytes/s) with 1 file(s) remainindownload: s3://preeti-demo
-bucket-2025-12-09/testfile.txt to ./downloaded.txt
```

Now you have a second copy called `downloaded.txt`, which came from S3.

8. Compute the Checksum of download file

Run : CertUtil -hashfile downloaded.txt SHA256

```
C:\Users\dell>CertUtil -hashfile downloaded.txt SHA256
SHA256 hash of downloaded.txt:
898393ccb6f176cc783e9417ad1af2453e7f9972ba64330c17166f6c0f655c8d
CertUtil: -hashfile command completed successfully.
```

```
C:\Users\dell>
```

You will get another long hash string.

9. Compare both checksums

If both checksums are IDENTICAL: **Your original file == Your S3 file**

That means:

- Integrity preserved
- No corruption
- No changes.

If they are DIFFERENT:

Something changed during upload/download.

The screenshot shows the AWS S3 console interface. The left sidebar has a tree view with 'Buckets' selected. The main area shows a table of 'General purpose buckets'. There are two buckets listed:

Name	AWS Region	Creation date
elasticbeanstalk-k-us-east-1-914471081680	US East (N. Virginia) us-east-1	October 16, 2025, 11:45:28 (UTC+05:30)
preeti-demo-bucket-2025-12-09	Asia Pacific (Mumbai) ap-south-1	December 9, 2025, 12:56:35 (UTC+05:30)

On the right, there are three cards: 'Account snapshot', 'External access summary - new', and 'Storage Lens'.

The screenshots show the AWS S3 console interface. The top screenshot displays the 'Objects' tab for the bucket 'preeti-demo-bucket-2025-12-09', which contains a single object named 'testfile.txt'. The bottom screenshot shows the detailed properties for 'testfile.txt', including the owner, AWS Region, Last modified date, Size, Type, Key, and various URLs.

Object	Properties
testfile.txt	Owner: cf1bc5f7a30c0a3786b534e8725e57b47ffd47de302de0cc27304702f947e9e AWS Region: Asia Pacific (Mumbai) ap-south-1 Last modified: December 9, 2025, 19:12:40 (UTC+05:30) Size: 26.0 B Type: txt Key: testfile.txt S3 URI: s3://preeti-demo-bucket-2025-12-09/testfile.txt Amazon Resource Name (ARN): arn:aws:s3:::preeti-demo-bucket-2025-12-09/testfile.txt Entity tag (Etag): c3d7ad57ebd48285ed15115a71be0e8 Object URL: https://preeti-demo-bucket-2025-12-09.s3.ap-south-1.amazonaws.com/testfile.txt

10. Conclusion

A checksum is a digital fingerprint of a file
SHA-256 produces a unique hash.

Uploading to S3 did not modify or corrupt the file
The fingerprints were identical.

This proves the file was transferred correctly
No corruption
No loss
No extra bytes
No changes

You manually performed a data integrity validation workflow
This is exactly what cloud engineers do for:
backups
database dumps
logs

software releases
migrations
forensics
a full integrity check successfully.

Now you understand Step 3 completely:

- ✓ Calculate checksum locally
- ✓ Upload file
- ✓ Download file
- ✓ Recalculate
- ✓ Compare

If they match → Integrity OK

- ❖ Understand how to make S3 store checksum metadata automatically
- ❖ Learn MD5 vs SHA256
- ❖ Do the same test with a larger file
- ❖ Try a corrupt file scenario to see mismatch
- ❖ Learn how to automate this with a script