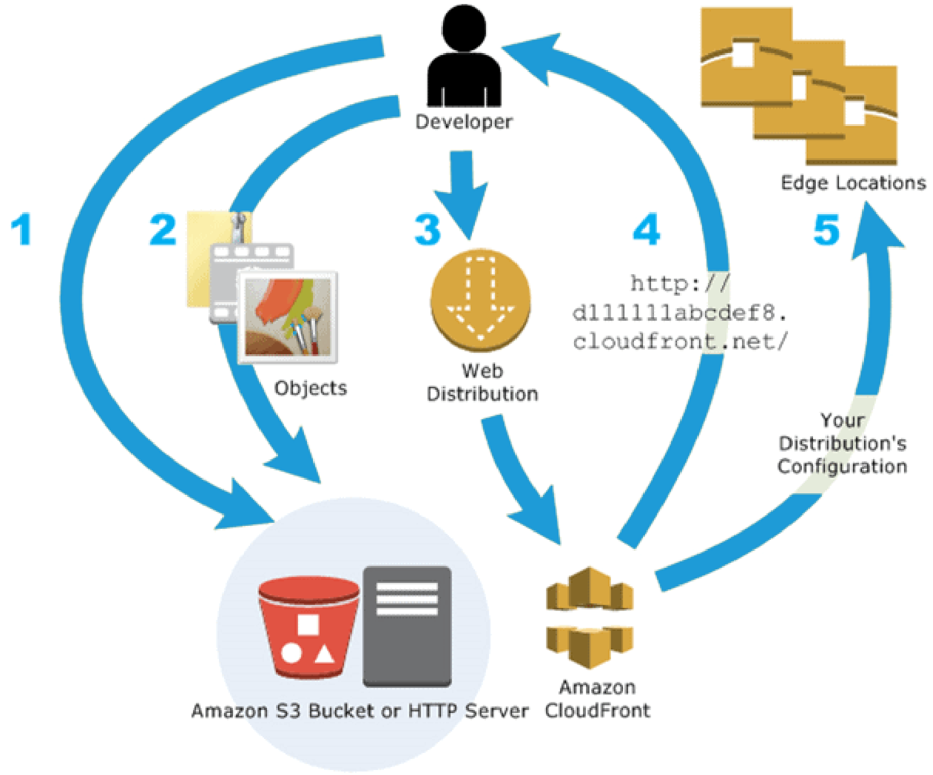
AWS CloudFront

AWS CloudFront is a fully managed, high-performance content delivery network (CDN) that accelerates the delivery of static, dynamic, and streaming web content to end-users.

AWS CloudFront

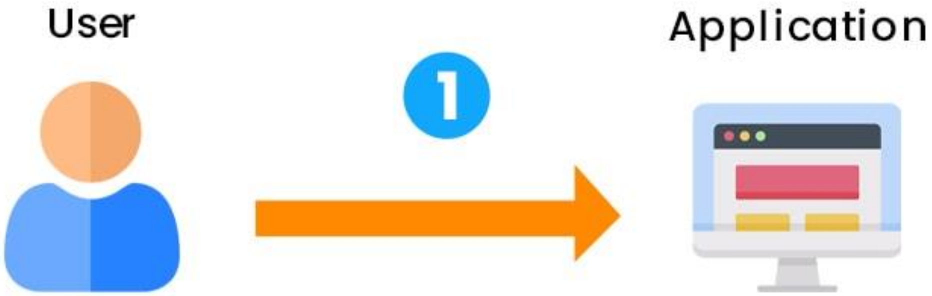
It is an Amazon Web Services globally dispersed network that distributes software, SDKs, videos, and other types of content to customers securely and quickly. It gives businesses and web application developers a simple and cost-effective way to distribute information with low latency and high data transfer speeds. It speeds up content delivery by routing each user request to the closest edge location that can best serve the content, resulting in the **shortest latency** (time delay).


Developer
Edge Locations
1
2
3
4
5
Objects
Web Distribution
http://d111111abcdef8.cloudfront.net/
Your Distribution's Configuration
Amazon S3 Bucket or HTTP Server
Amazon CloudFront

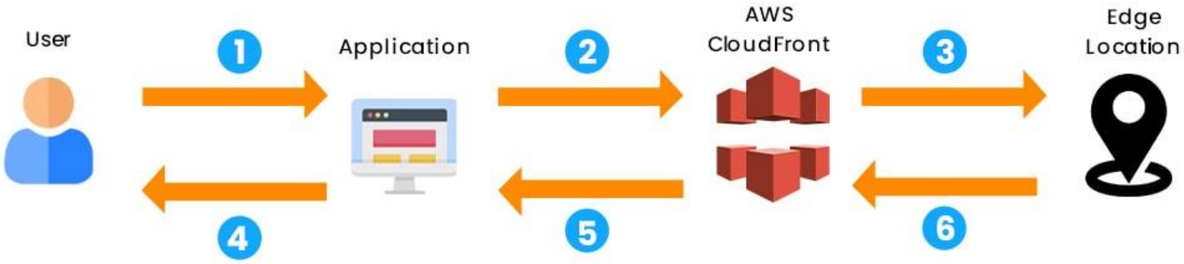
How Does AWS CloudFront Work?

The following steps describe how CloudFront delivers content:

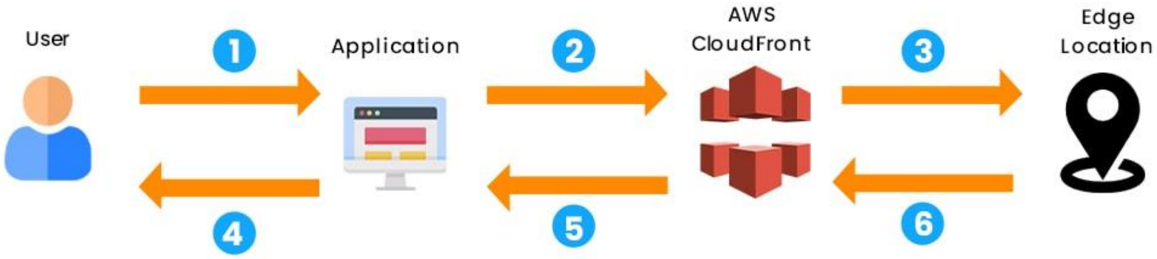
Step 1: The client visits a website and requests that a file is downloaded (like an image file).



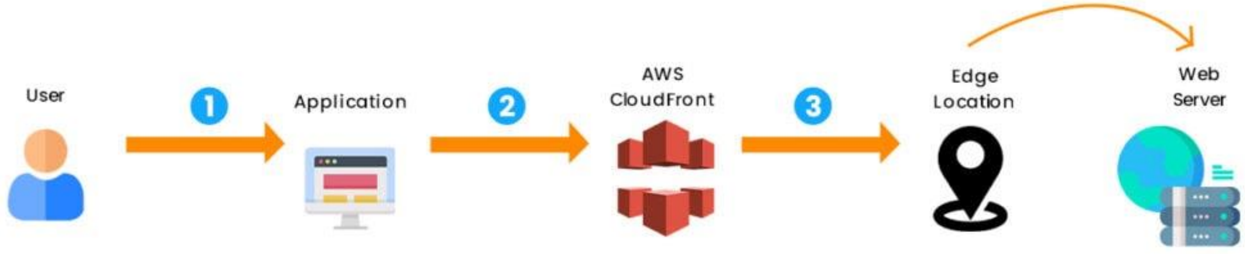
Step 2: The DNS now routes the client request to the nearest edge location via CloudFront to serve the user request.



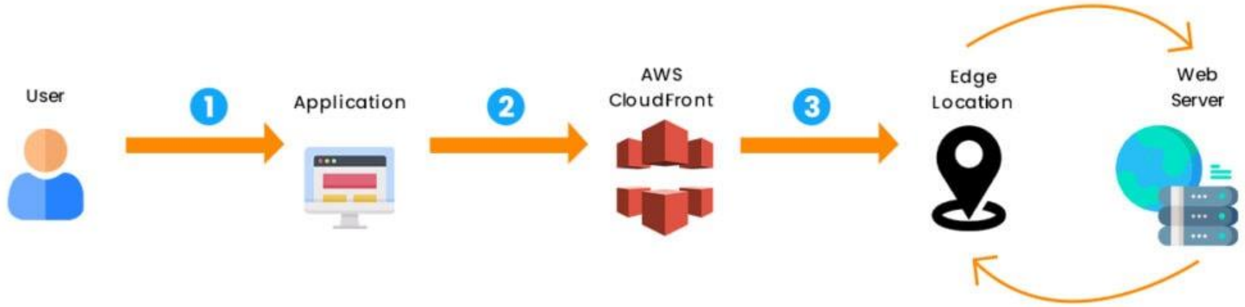
Step 3: It searches for the requested cache file at the edge location. When a file is found, CloudFront sends it to the user.



Step 4: If the file is not found, CloudFront compares the requirements to the specifications and shares it with the appropriate server.



Step 5: The web server sends the files back to the CloudFront edge location in response to the request.



Step 6: When CloudFront receives the file, it immediately shares it with the client and adds it to the edge location.

Benefits of AWS CloudFront

- It's easy to use and ensures higher productivity.
- It improves reliability and availability by storing copies of objects in multiple edge locations worldwide.
- Because of the '*Content Privacy'* feature, it has a high level of security.
- To deliver content quickly, it employs HTTP or HTTPS protocols.
- It has the most advanced security features, including field-level encryption and HTTPS support.

Use Cases of AWS CloudFront

1. Accelerate the delivery of static website content: It can accelerate the delivery of static content (such as images, style sheets, JavaScript, and so on) to viewers worldwide. You can use it to take advantage of the AWS backbone network and CloudFront edge servers to provide your website visitors with a fast, safe, and dependable experience.
An Amazon S3 bucket is a straightforward method for storing and delivering static content. Using S3 in conjunction with CloudFront has several benefits, including using Origin Access Identity (Oeasily AI) to restrict access to your S3 easily.

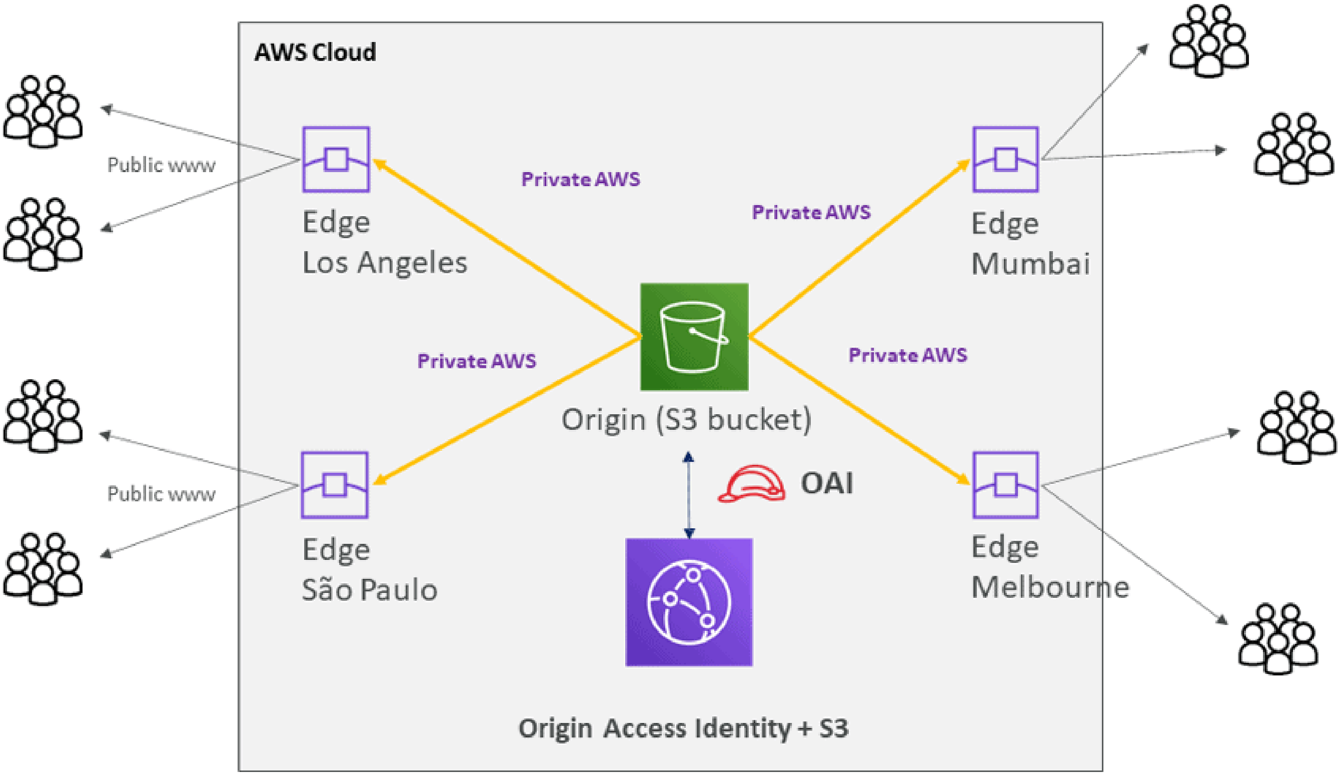
2. Serve video on demand or live video streaming: It provides various options for streaming your media to global viewers, including pre-recorded files and live events.

- It can stream video on demand (VOD) to any device in standard formats such as MPEG DASH, Apple HLS, Microsoft Smooth Streaming, and CMAF.

- To reduce the load on your origin server when broadcasting a live stream, you can cache media fragments at the edge. Multiple requests for the manifest file that delivers the fragments in the correct order can be combined.

3. During the system processing, encrypt specific fields: You have secure end-to-end connections to origin servers when configuring HTTPS with CloudFront. In addition to HTTPS security, field-level encryption allows you to protect specific data throughout system processing so that only certain applications at your origin can see it. To enable field-level encryption, add a public key to CloudFront and specify the set of fields to be encrypted with the key.

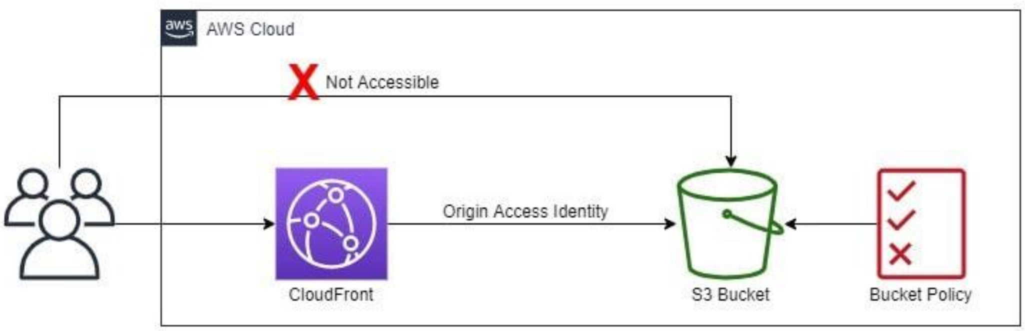
4. Customize on the fly: Running serverless code at the edge opens up new avenues for customising content and experiences for viewers while reducing leasing Lambda@Edge with CloudFront, allowing you to customise the content that CloudFront delivers in a variety of ways. When your origin server is down for maintenance, you can return a custom error message so that viewers do not see a generic HTTP error message.



AWS CloudFront with S3

- The content from an S3 bucket can be distributed using it.
- The advantages of using CloudFront over S3 are as follows:
  - CloudFront data transfer can be more cost-effective if the objects are frequently accessed because CloudFront data transfer is much lower than the price for S3 data transfer at higher usage.
  - Because the objects are stored closer to the users, downloads are faster with CloudFront than with S3 alone.
- Because public read permissions must be granted to S3 origin objects, they are accessible from S3 and CloudFront.
- Even though CloudFront does not reveal the underlying S3 URL, the user will be aware of it if it is shared directly or used by applications.
- It would be necessary to prevent users from having direct access to the S3 objects when using CloudFront signed URLs or signed cookies to provide access to them.

- The **Origin Access Identity** (OAI) can be used to prevent users from directly accessing S3 objects.



- The distribution can be associated with an origin access identity, a particular CloudFront user.
- S3 bucket/object permissions must be set only to allow access to the Origin Access Identity.
- When users access the object through CloudFront, the OAI retrieves the content on their behalf, whereas direct access to the S3 object is restricted.

Security for AWS CloudFront

1. It supports Encryption in Transit and can be configured to require viewers to use HTTPS to request files, ensuring that connections are encrypted when CloudFront communicates with viewers.
2. It offers encryption at Rest.
3. Restricting content access
    - To restrict access for specific users, use signed URLs or cookies.
    - Create a web access control list (web ACL) with AWS WAF web ACLs to restrict access to your content.
    - Geo-restriction, also known as geoblocking, prevents users in specific geographic locations from accessing content served by a CloudFront distribution.
    - To prevent users from using the file’s direct URL, restrict access to content in S3 buckets using origin access identity – OAI.

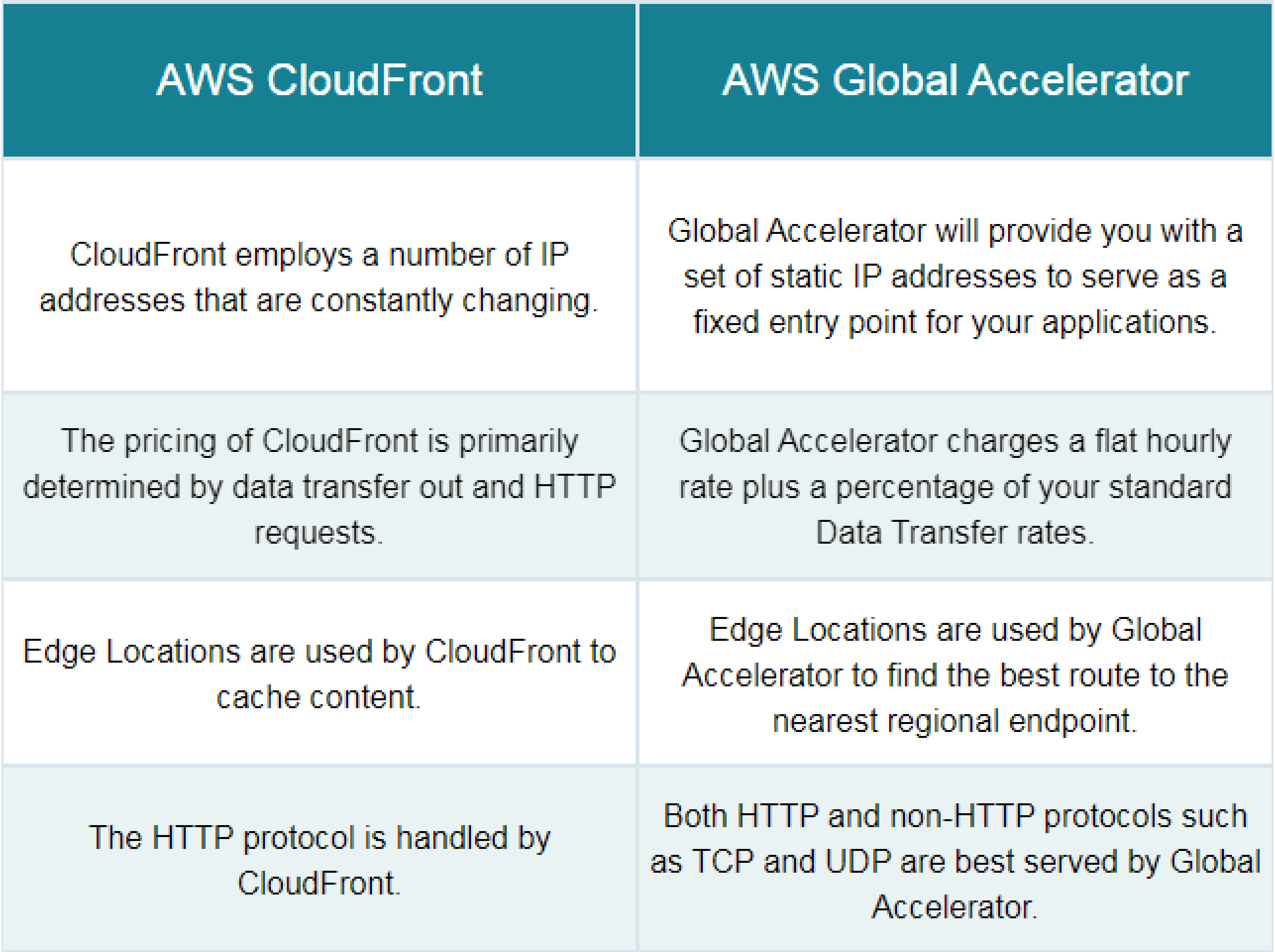
AWS CloudFront Pricing

Charges for CloudFront are calculated based on actual usage in four areas:

- **Outbound Internet Data Transfer**
    - Charges are assessed based on the amount of data transferred from CloudFront edge locations, measured in gigabytes (GB).
    - Data transfers from AWS origin (e.g., S3, EC2, etc.) to CloudFront are no longer charged. This applies to data transfers from all AWS regions to global CloudFront edge locations.
- **Requests made via HTTP/HTTPS**
    - The total number of HTTP/HTTPS requests for the content.
- **Invalidation Requests**
    - Invalidation request per path

  - The URL (or multiple URLs if the path contains a wildcard character) of the object you want to invalidate from the CloudFront cache is represented by a path listed in the invalidation request.
- **Dedicated Internet Protocol (IP) Custom SSL certificates that are linked to a CloudFront distribution**
  - $600 per month, pro-rated by the hour, for each custom SSL certificate associated with one or more CloudFront distributions that use the Dedicated IP version of custom SSL certificate support.

AWS Global Accelerator vs Amazon CloudFront



AWS CloudFront	AWS Global Accelerator
CloudFront employs a number of IP addresses that are constantly changing.	Global Accelerator will provide you with a set of static IP addresses to serve as a fixed entry point for your applications.
The pricing of CloudFront is primarily determined by data transfer out and HTTP requests.	Global Accelerator charges a flat hourly rate plus a percentage of your standard Data Transfer rates.
Edge Locations are used by CloudFront to cache content.	Edge Locations are used by Global Accelerator to find the best route to the nearest regional endpoint.
The HTTP protocol is handled by CloudFront.	Both HTTP and non-HTTP protocols such as TCP and UDP are best served by Global Accelerator.