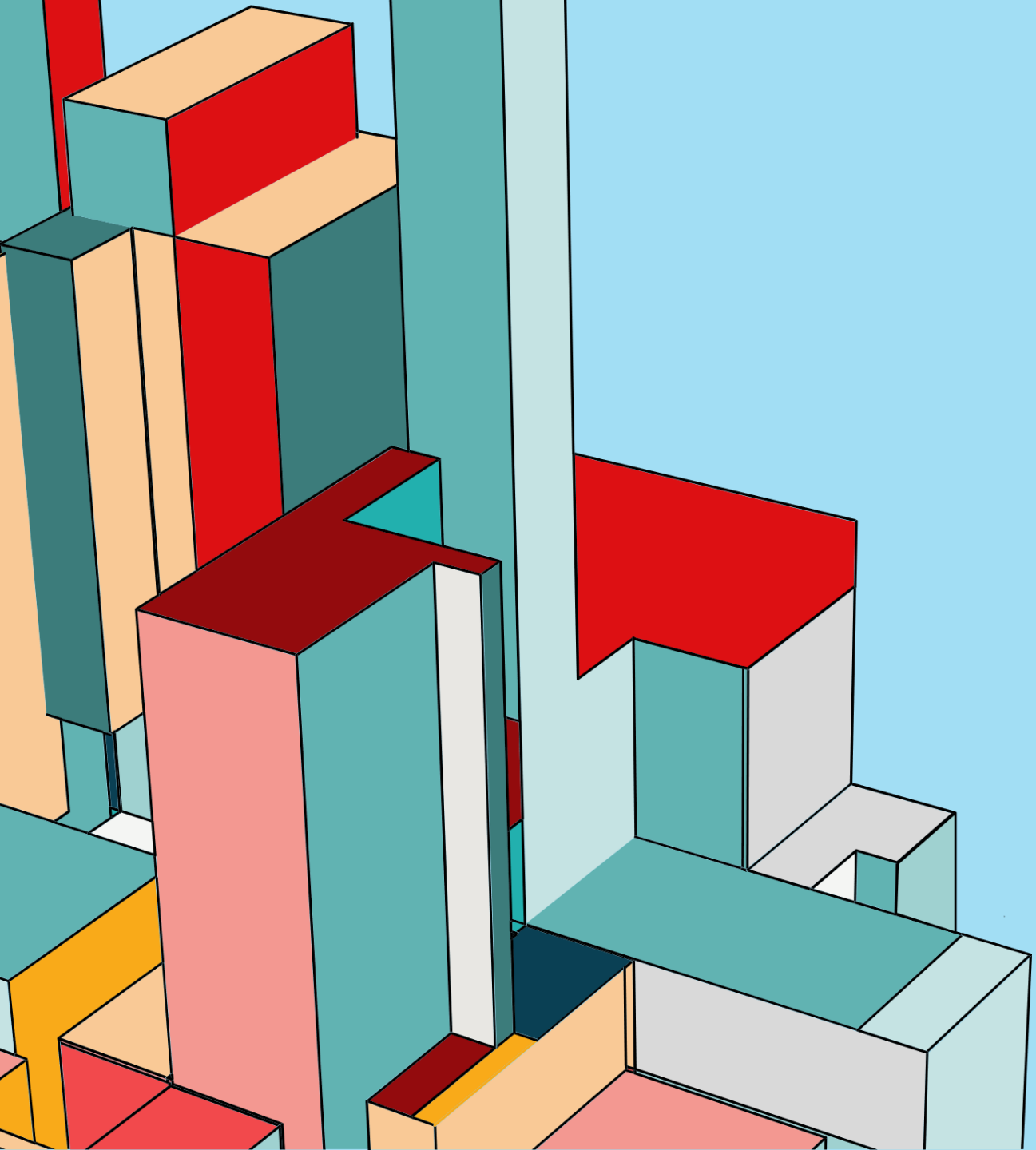


DEPLOYING A FULL-STACK APP ON aws

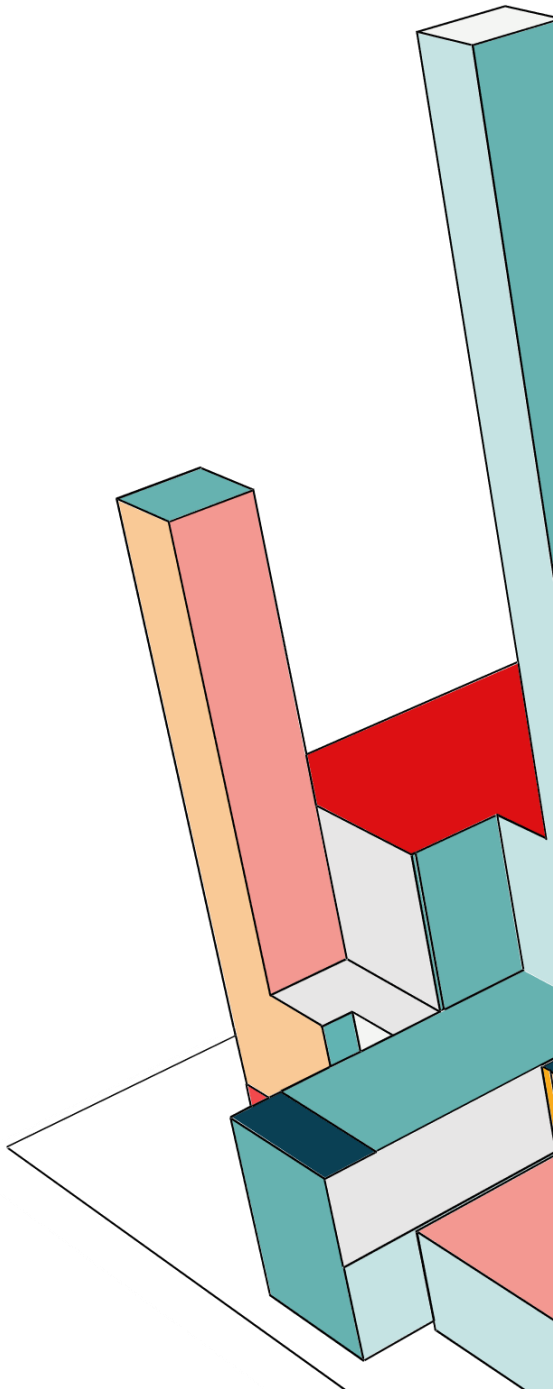
CONTENTS

INTRODUCTION

Deploying your app on aws has never been easier. But before we begin, here are some basic terminology that you may need to be acquainted with as they will be used during this session.

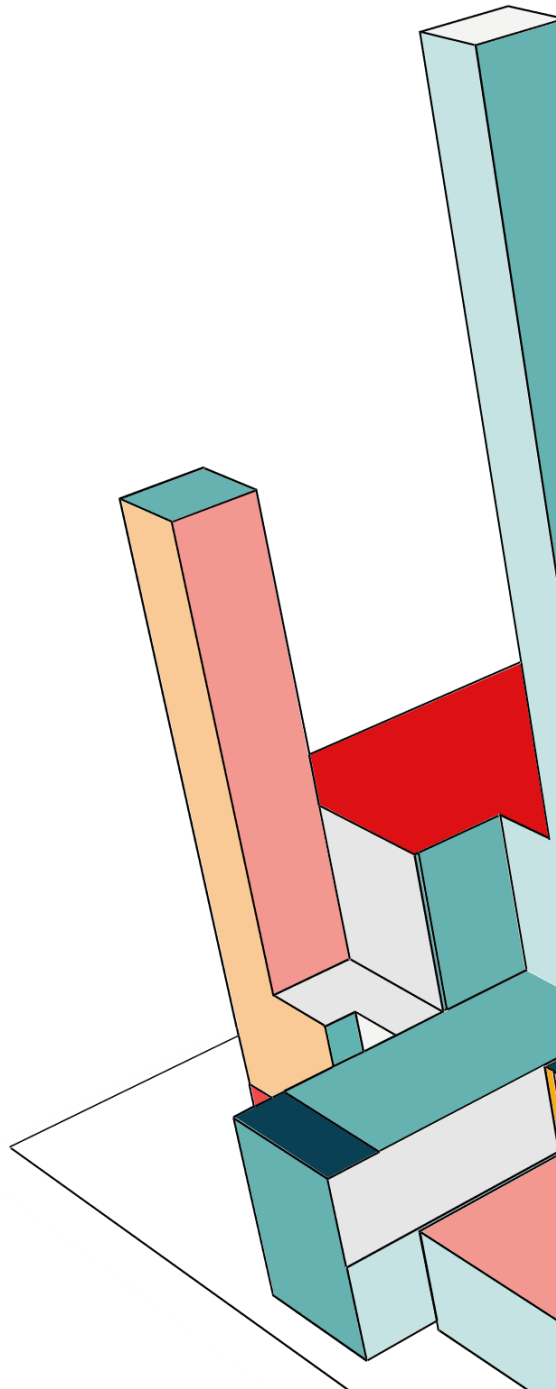
BRIEF DEFINITION OF TERMS

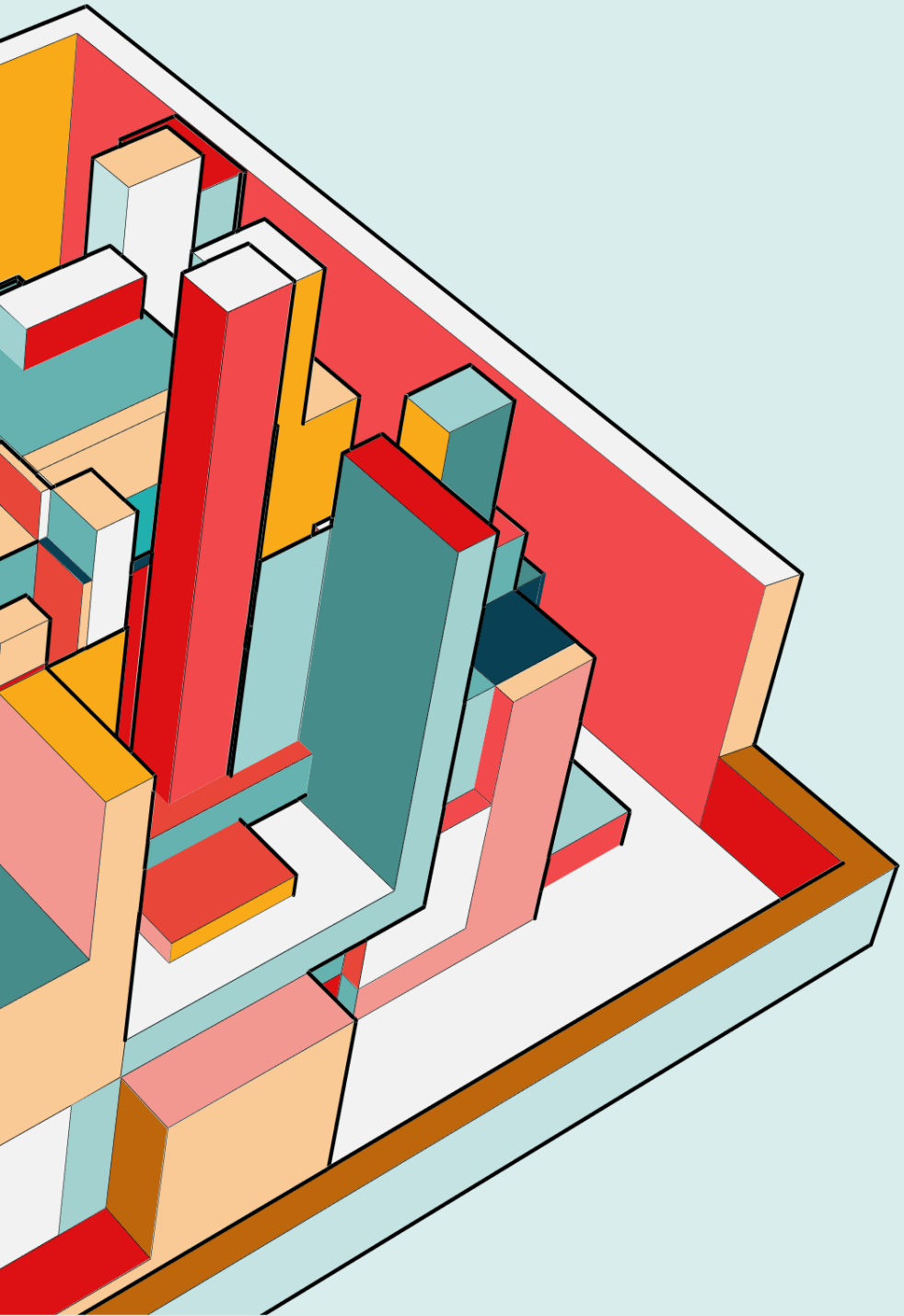
- Virtual Private Cloud (VPC): VPC is a network created for your project or organization in aws. VPC will handle the network requirements e.g subnets and ip addresses for your resources.
- CloudFront – A service that speeds up content delivery by caching data at edge locations worldwide
- Route 53 - performs domain registration, DNS routing and health checks
- Simple Standard Storage (S3) – AWS native storage solution.
- Identity Access Manager (IAM) – IAM controls who has access to what resource(s)



BRIEF DEFINITION OF TERMS

- Elastic Compute Cloud (EC2) – this service provisions a virtual computer instance which will serve as our server.
- Availability Zone – this shows the presence of an aws datacenter within a region. The closer you are to an AZ, the faster your data can be transferred (low latency)
- Cloud Trail – AWS tool to monitor latency between your resources.
- Security Group – controls network access to your resource eg EC2 instance





DEPLOYMENT PROCESS

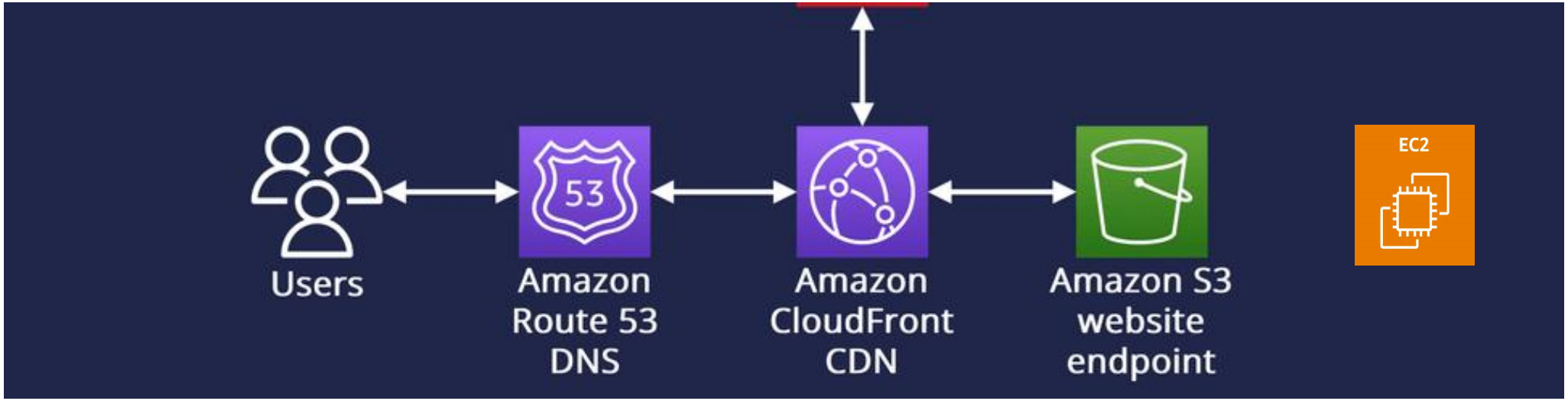
This covers an overview on the deployment process. We'll go through the flow process starting from:

User → Route 53 → CloudFront → S3 → EC2

DESIGN FLOW

User → Route 53 → CloudFront → S3 → EC2

IAM and Security Groups will be used to secure user and network access, and resources can be distributed across availability zones.



SERVICE BREAKDOWN

Route 53

Route 53 acts as the Domain Name System (DNS) for your domain (e.g., `aws-uniuyo-club.com`). It performs domain registration, DNS routing and health checks.

When a User enters www.aws-uniuyo-club.com on his browser, Route 53 resolves the domain and routes the traffic.
Route 53 can route traffic directly to:

- A CloudFront distribution (CDN)
- An Application Load Balancer (ALB)
- An EC2 public endpoint
- An S3 bucket (for static hosting).

CloudFront (CDN Layer)

CloudFront manages caching of data at edge locations around the world to help improve content distribution to users. It basically stores a copy of your data and forwards this to the user upon request instead of always placing a request to your backend.

CloudFront can cache data from an S3 bucket (static site, images, JS, CSS, videos), ALB or EC2 instance (dynamic content, APIs).

User request → CloudFront edge location. If cached: served immediately, If not cached: CloudFront fetches from origin (S3, EC2, or ALB).

SERVICE BREAKDOWN

EC2 Instances (Compute Layer)

EC2 instance is a virtual computer that can run web servers, applications, or APIs. It can be:

- Launched inside a VPC.
- Spread across subnets (public or private).
- Public-facing or a private instance.

Requests (from CloudFront) → reach EC2 instances, EC2 responds with dynamic data or static files stored on S3.

S3 Buckets (Storage Layer)

Simple standard storage (S3) is AWS' native cloud storage solution. Can be divided into classes such S3 standard (regularly accessed data) and S3 glacier (rarely accessed data archive).

- S3 is used to store media/files, backups, logs, or even host static websites.
- Serves as CloudFront origin for static assets.

CloudFront fetches static files → caches them globally. EC2 can read /write to files stored in S3 when an endpoint is triggered and the output is forwarded to the user who made the request.

SECURITY: IAM ROLES AND NETWORK SECURITY

IAM Roles

IAM controls which user or service is allowed to use a specific resource in your AWS organisation.

- EC2 instance may need IAM roles granting S3 access.
- CloudFront can be granted an Origin Access Identity (OAI) role to securely fetch from S3.

Best Practice

- Apply principle of least privilege when granting an IAM role to a user or service. Only grant it the specific role(s) it needs and nothing more.
- Create a group, bind the IAM role to the group, then add the specific users or service accounts to the group.

Security Groups

Security groups control inbound/outbound traffic for your EC2 instance or ALB. They contain firewall rules which control the specific ip ranges and ports can be used to access the EC2 instance (ingress rules) and the same for your EC2 instance outbound traffic (egress rules)

Network Encryption

- HTTPS (TLS) for data in transit.
- S3 server-side encryption (SSE-S3, SSE-KMS).
- Encrypted EBS volumes for EC2.

SUMMARY

- Setup S3 bucket and EC2 instance with proper permissions
- Setup Route 53 and Cloudfront configurations
- Deploy Static Frontend (GitHub → S3)
- Deploy API backend (GitHub → EC2).
- Connect S3 bucket to EC2 instance.
- Test and monitor connection with Cloudtrail.

Seek feedback

Reflect on performance

Explore new techniques

Set personal goals

Iterate and adapt

FAQS

1. Can I setup a full-stack app in EC2 without using S3?
2. Is AWS expensive to use?
3. Can I migrate a pre-existing full-stack app to AWS?

YOU ARE AWESOME THANK YOU!

You can reach out to me via email or linkedIn. The resources for this session will be in the github repo below.

okekechiletaram@gmail.com

linkedin.com/in/chilet

github.com/chilet-okeke/aws_deployment.git