Smart Door System – Technical Documentation

Overview :

The Smart Door System is a cloud-driven security application designed to identify visitors using Amazon Rekognition and grant access through One-Time Passcodes (OTPs). The system handles both known and unknown visitors, providing a seamless and secure flow using several AWS services including Lambda, DynamoDB, Kinesis Video Streams, SNS, S3, and API Gateway.

Architecture Summary :

The system consists of four major components:

1. Video Ingestion

- A camera streams real-time video using RTSP.
- Video is pushed to **Amazon Kinesis Video Streams (KVS)**.
- Rekognition continuously analyzes the stream for faces.

2. Face Detection & Matching

- Rekognition matches detected faces against a **Face Collection**.
- If a known face appears, a **Kinesis Data Streams (KDS)** record is produced containing:
  - FaceID
  - Confidence
  - Timestamp
  - Bounding box
  - ExternalImageID (stored name)

3. Lambda Event Processing

Three Lambda functions handle workflow automation:

a. smartdoor-lf1

Triggered by KDS.

- If visitor is known → generates OTP, stores in DynamoDB, sends via SNS.

b. smartdoor-verify-otp

Called from the S3-hosted web page.

- Validates OTP stored in DynamoDB.
- Responds with access granted/denied.

c. smartdoor-register-visitor

Invoked when an *unknown* visitor link is opened.

- Owner enters visitor name + note.
- Generates OTP + stores entry + sends email.

4. Visitor Interaction Web Pages (S3 + API Gateway)

- **WP1 – Unknown Visitor Approval Page**
  - Hosted in S3 as a static site.
  - Owner enters visitor details.
  - Triggers Lambda to issue OTP.

- **WP2 – Virtual Door Page**
  - Visitor enters OTP.
  - API Gateway → Lambda → DynamoDB checks OTP.
  - Displays result.

Data Storage Design :

- **DynamoDB – Visitors Table**

  Partition key: faceId
  Attributes:

  - name
  - phoneNumber
  - photos (list of maps: bucket, objectKey, timestamp)

- **DynamoDB – Passcodes Table**

  Partition key: otp
  Attributes:

  - faceId
  - timestamp
  - ttl (Time To Live – auto deletion)

Notification Workflow (SNS) :

SNS sends:

- OTP messages to known visitors
- Unknown visitor alerts to owner email
- Approval page link appended to message

Security Considerations :

- AWS credentials never stored client-side.
- IAM least privilege applied.
- OTP stored with TTL to auto-expire.
- No secrets committed in GitHub.
- S3 sites public *only for hosting HTML*, not for storing sensitive data.

Technologies Used :

- AWS Lambda (Python)
- Amazon Rekognition
- Amazon Kinesis (Video & Data Streams)
- Amazon S3 Static Hosting
- Amazon SNS
- Amazon DynamoDB
- API Gateway HTTP APIs
- MediaMTX / FFmpeg for RTSP simulation
- Docker for streaming container

Conclusion :

This project successfully integrates multiple AWS serverless and AI services to create a functional smart-door security system. The architecture is scalable, event-driven, and secure, showcasing practical use of cloud-native design patterns.