ChatBot HLD + LLD Architecture

Public Zone

MFA, Password Policies
MDM, CA Policy
Oauth/OIDC, SSO

Authenticated user

Front-End Web & Mobile

AWS Identity and Access Management (IAM)

TLS encryption

Rate limiting, Session Control
Mutual TLS (mTLS)
Input Validation & Filtering

API Gateway

Web Application Firewall

Application Zone

IAM Roles (RBAC, ABAC)
VPC/Subnet, Private Links
NSGs, ASGs

Chatbot Application

AWS Identity and Access Management (IAM)

Mutual TLS (mTLS)

Model Zone

IAM Policies, RBAC, ABAC
VPC/Subnet, Private Links
NSGs, ASGs

Amazon Bedrock

AWS Identity and Access Management (IAM)

Queries

Prompts

Embedding Model

Large Language Model

Retrieves

Stores Embeddings

Data Zone

TLS encryption

Amazon Aurora

Encrypted RDS
Row-Level / Column-Level Security
S3 Access Logs
IAM Policies, RBAC, ABAC
VPC/Subnet, Private Links
NSGs, ASGs

Amazon Simple Storage Service (Amazon S3)

AWS Identity and Access Management (IAM)

Encrypted by KMS

Logs to CloudTrail

Store credentials, API keys

AWS Key Management Service (AWS KMS)

AWS CloudTrail

AWS Secrets Manager