# Week 4 Notes and Resources

## Key Concepts

### Amazon Cognito User Pools

Create and maintain a user directory and add sign-up and sign-in to your mobile app or web application using user pools. User pools scale to hundreds of millions of users and are designed to provide simple, secure, and low-cost options for you as a developer.

You can use user pools to add user registration and sign-in features to your apps. Instead of using external identity providers such as Facebook, or Google, you can use user pools to let users register with or sign in to an app using an email address, phone number, or a user name.

Amazon Cognito User Pools are compliant with SOC 1-3, PCI DSS, ISO 27001, and is HIPAA-BAA eligible.

For more see Amazon Cognito User Pools

## AWS Certificate Manager

AWS Certificate Manager (ACM) can help you deploy your SSL/TLS Certificates to your AWS infrastructure such as the Application Load Balancer. If you don't have a certificate, ACM can issue you a certificate as well.

For more see What is AWS Certificate Manager

## Securing the connection between your Users and Your Load Balancer

You can create a listener that uses encrypted connections (also known as SSL offload). This feature enables traffic encryption between your load balancer and the clients that initiate SSL or TLS sessions.

For more see HTTPS Listeners for Your Application Load Balancer

## Encrypting Data in AWS

Encrypting data in Transit:

- Configure Apache Webserver on Amazon Linux to Use SSL/TLS from EC2 User Guide
- Since we are using NGINX you may find this link helpful from eff.org helpful as well
- Using SSL to Encrypt a Connection to a DB Instance

Encrypting Data at Rest:
* For encrypting storage volumes for your EC2 Instances, see Amazon EBS Encryption

- For encrypting your RDS database, see Encrypting Amazon RDS Resources

- For encrypting S3 content, see Amazon S3 Default Encryption for S3 Buckets and AWS S3 Encryption.

- If you'd like to take more control of the encryption keys with AWS KMS see How AWS Services use AWS KMS

For more on encrypting your data on AWS, see AWS Security Blog on Encryption

## AWS Compliance Programs

If you handle sensitive customer data in your applications, please review specific materials at AWS Compliance Programs

You may also learn more about Security in the AWS Cloud by reviewing the AWS Security Whitepaper

## Bonus

## Using Cognito User Pools SDK to Update User Attributes

Using the SDK for the Cognito Identity Provider, you can call admin_update_user_attributes method to modify user attributes in the user directory.

### Resources for Optional Amazon Polly Challenge

Amazon Polly is a service that performs Text-to-Speech.

You may want to review the Boto3 Amazon Polly reference docs.

## What you accomplished this week

- You created a user directory using Cognito User Pools
- You integrated user authentication and authorization into the application
- You learned about options for securing the data in transit and at rest for the application