

# StorePot: One Stop Storage Solution

Project: StorePot: One Stop Storage Solution

University Name: <http://www.sjsu.edu/>

Course: CMPE(281) – Cloud Technologies

Professor: Sanjay Garje

ISA: Rajalakshmi Babu

Student: Sneha Patil (SJSU Id: 013942006)

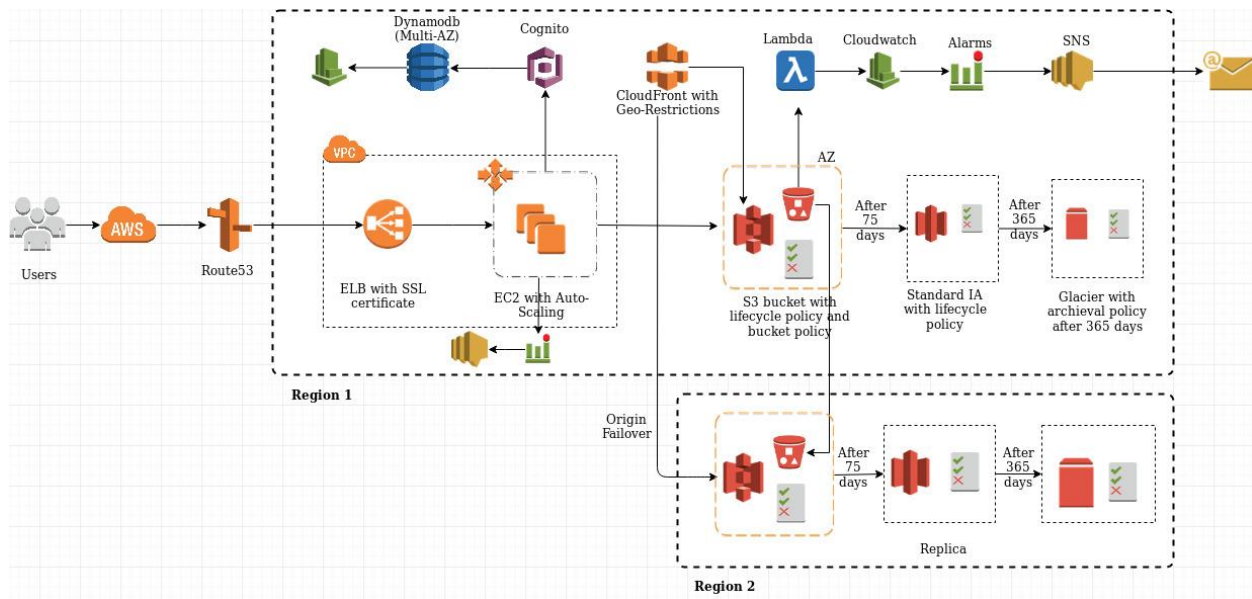
## Introduction:

StorePot is a 3tier web application hosted on AWS cloud which intend to provide platform for the Authorized users to maintain their file storage. The application is made highly available, scalable and cost effective using different AWS components. This application leverages the AWS Cognito for authentication and authorization of users. The application has been deployed on EC2 which offers auto-scaling along with Elastic Load Balancer which will automatically distribute traffic to multiple EC2 instances. Dynamodb has been used as a storage system for storing details of files stored in AWS S3. Amazon S3 has been used for storing files while Cloudfront service has been leveraged to download the file. To make the storage more secure, Lambda is used which will trigger whenever a file is deleted from S3 bucket. Lambda will log the event in cloudwatch and SNS will send an email notification based on cloudwatch alarm settings.

## Activities Users can perform:

1. Browse through already uploaded file.
2. Upload new file with description
3. Update the already uploaded file
4. Delete the file uploaded.

## Solution Architecture:



### StorePot Features:

1. Home page has SignIn option where user is authenticated using AWS Cognito. For the new user, SignUp functionality is provided.
2. User can also login into the system using social logins like "Login using Facebook" and "Login using Google"
3. There is a "admin" group created in AWS Cognito and only admin users are added to that group. Based on the user's role, user will be redirected to appropriate page.
4. Login details for all the users will be stored in Cognito.
5. Logged in user can upload a new file, browse through already uploaded files and download or delete the uploaded file.
6. Admin user has access to all the files uploaded by all the users and can download and delete the files.
7. File uploaded by authorized users will be stored in S3 bucket and file size cannot exceed 10MB size.
8. Authorized users can download files uploaded to S3 via cloudfront.
9. The user's file details are stored in DynamoDB

### AWS Components Leveraged:

1. Route53: Web application is accessible over internet through the hosted domain. This hosted domain is registered with Route53.
2. Elastic load balance: Certbot SSL certificate is deployed on elastic load balancer. Load would be distributed accordingly to target groups.
3. EC2 with Auto Scaling: React and Nodejs application are deployed on EC2 where auto scaling is enabled based on CPU utilization.

4. AWS Cognito: For user Authentication and authorization.
5. Amazon S3: Highly available and scalable solution used for uploading and storing user's files.
6. Standard IA: Lifecycle policies are set to S3 bucket to move files from S3 to standard IA after 75 days.
7. Amazon Glacier: Lifecycle policies are set to bucket to move files from standard IA to Glacier after 365 days.
8. CloudFront: To reduce the load on S3 origin, cloudfront has been leveraged during file download. Minimum TTL has been set to 1sec.
9. DynamoDB: To store the uploaded file details. DynamoDB is automatically replicated across multiple availability zones providing high availability and durability. For DR measures of DynamoDB, DynamoDB Global tables can be used for multi-region replication
- 10.** Lambda: The lambda function will be triggered if the file is deleted from S3 and event will be logged in CloudWatch.
11. CloudWatch & CloudWatch Alarms: Cloudwatch will log the S3 file delete event and alarm is set to send the SNS notification if the logs are there.
12. SNS: Email notification will be sent if the file is deleted from Amazon S3.