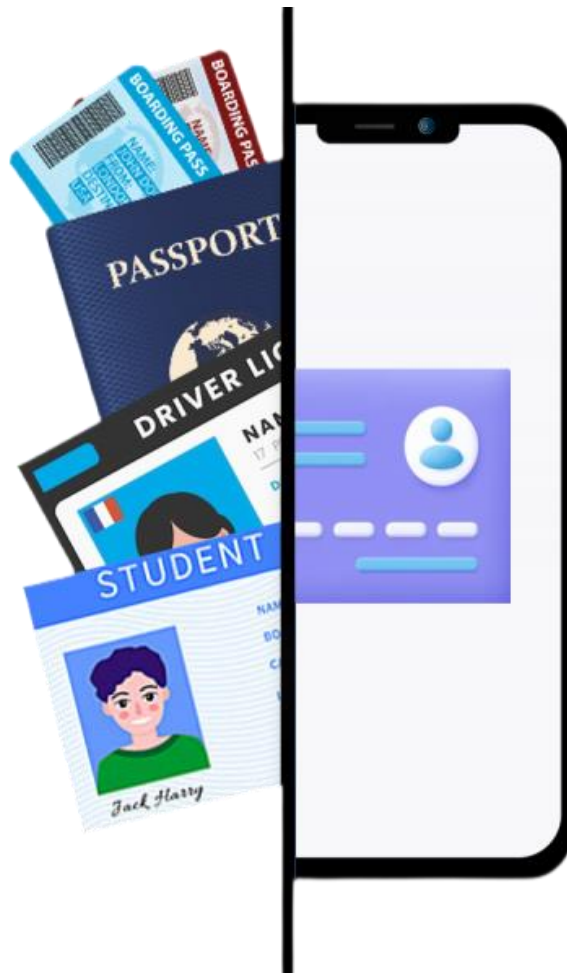


# CMPE-281- CLOUD TECHNOLOGIES

PROJECT #2: COMPONENT 2

## ONE-D: UNIQUE ID TO YOUR TRUE IDENTITY



SUBMITTED BY:  
ANANDU SREEKUMAR | JESWANTH VADLAMUDI | G SAI KRISHNA  
MASTERS IN COMPUTER SOFTWARE ENGINEERING  
SAN JOSE STATE UNIVERSITY

# INDEX

## 1. Introduction

1.1 Project Overview .....	3
1.2 Objectives and Goals .....	3
1.3 Motivation .....	4
1.4 Scope and Limitations.....	4

## 2. System Architecture

2.1 High-level overview of System Components and Walkthrough .....	5
2.2 Entity Relationship Diagram of databases used .....	7

## 3. User Manual

3.1 For User.....	8
3.2 For Notary Official.....	9

## 4. Technical Documentation:

4.1 Technologies Used .....	10
4.2 Screenshots .....	11
4.3 AWS Services Integration .....	16
4.4 Cloud Best Practices .....	22
4.5 CI/ CD Pipeline .....	24

## 5. Security Measures

5.1 Authentication and Authorization Mechanisms .....	25
5.2 Handling and Storage of Sensitive Information .....	26

## 6. Verification Process

6.1 Detail the steps involved in the verification process with the notary body .....	27
--	----

## 7. Scalability and Future Improvements

7.1 How the system can scale with an increasing user base .....	29
7.2 How the verification methods can be improved .....	29

## 8. Conclusion:

8.1 Summary of the project .....	30
8.2 Lessons learned .....	30

## 9. References .....

## 10. Individual Contributions, Test Credentials, AWS Costs.....

Project URL: <https://www.one-d.cloud> Code Repository Link: <https://github.com/AnanduSreekumar/ONE-D>

# 1. INTRODUCTION:

## 1.1 Project Overview:

**Problem Statement:** International students and travelers often face challenges in maintaining original copies of essential documents whether user check into a hotel, going to a movie theater, school or traveling abroad. The lack of these crucial documents can lead to various challenges and inconvenience, pointing towards a need of a reliable, secure, and easily accessible method of carrying and representing these documents.

**Proposed Solution:** “ONE-D”, a unique digital platform that acts as a universal virtual ID card, replacing the need to carry physical documents. This platform serves as a secure digital storage unit for users’ essential documents, mitigating the risks and inconveniences associated with forgetting or losing physical documents. ONE-D is not just a storage solution; it also collaborates with local verification bodies (like notaries from UPS) to authenticate the digitally stored documents. When users upload their documents, the system generates questions that are subsequently verified by a local verification body. This step is vital as it authenticates the digital copy, ensuring it’s recognized and accepted as a valid form of identification or documentation globally. Users are assigned a unique ID, which they can present for verification. Additional security is added through a one-time password system, valid for a day, ensuring that information access is timely and secure. Additionally, users can share their information via NFC by tapping their phone and VIP users benefit from physical cards with RFID technology, further simplifying the verification process. With ONE-D, carrying multiple physical documents and worrying about losing documents becomes a thing of the past.

## 1.2 Objectives and Goals:

The primary objective of the One-D System is to completely eliminate the dependence on physical ID cards, thereby mitigating the associated risks of loss, theft, and forgery. This overarching goal is complemented by a set of secondary objectives, including the streamlining of identity verification through a notary body and the facilitation of secure check-ins at third-party establishments using the generated One-D.

Beyond these primary and secondary goals, the project aspires to redefine the user experience within the realm of identity management. By introducing a user friendly, secure, and digitized process, One-D positions itself at the forefront of the ongoing digital transformation in the field of identity verification.

### 1.3 Motivation:

The motivation driving the development and implementation of the One-D System arises from the vulnerabilities and inconveniences associated with physical ID cards. These cards are susceptible to various risks, including loss, theft, and forgery, leading to identity-related fraud and security breaches. The One-D System addresses these concerns directly by digitizing the identification process, offering a secure and highly efficient alternative.

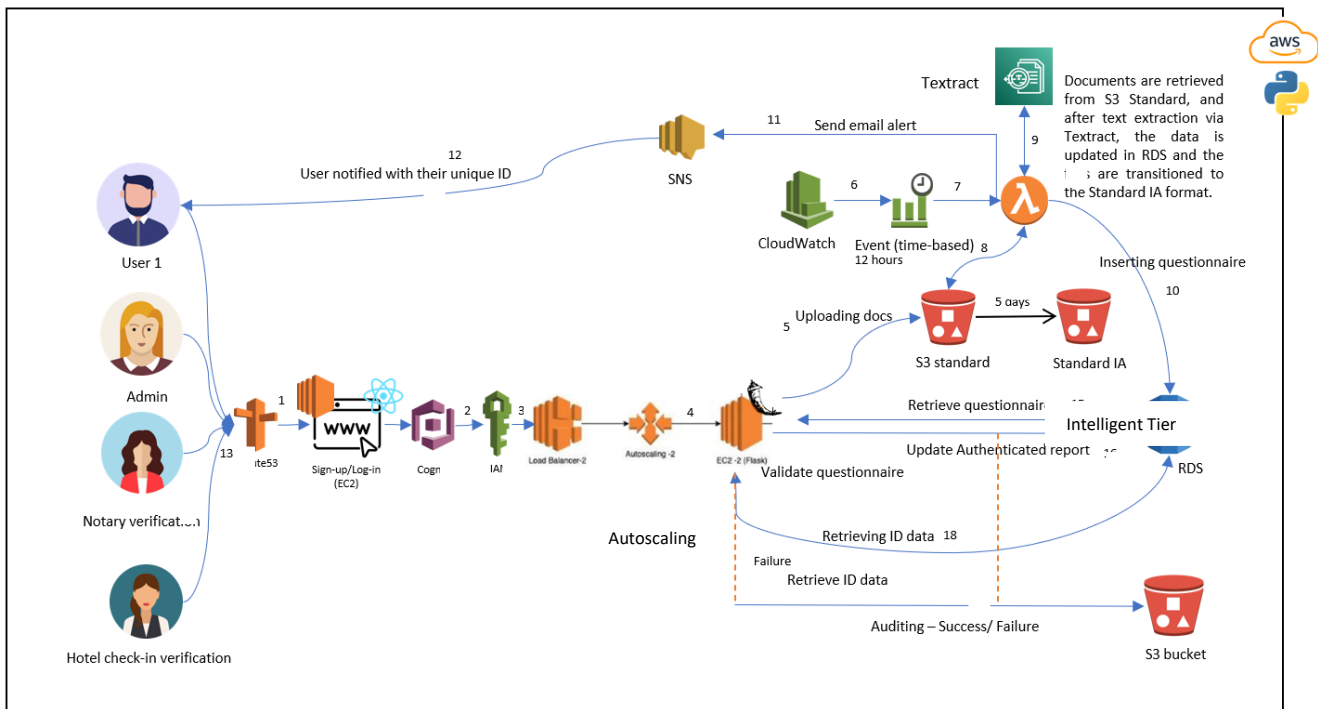
Furthermore, the project's motivation extends to enhancing user convenience. Traditional identity verification processes can often be perceived as time-consuming and cumbersome. In response, One-D leverages cutting-edge technology to streamline these processes, providing users with a highly intuitive, user-friendly, and efficient experience.

### 1.4 Scope and Limitations:

The scope of the One-D System encompasses the entire lifecycle of identity management for users. From the initial user sign-up to the verification process facilitated by a pre-approved notary body, and through the subsequent use of the generated One-D for third-party interactions, the system aims to provide a holistic, end-to-end solution.

While the system's capabilities are extensive, it is equally important to acknowledge its limitations. The One-D System does not govern the initial issuance of government identity cards; instead, it relies on the assumption that the notary body verification process is conducted with integrity. Recognizing these limitations is crucial as they delineate the system's boundaries and highlight areas where collaboration with existing processes is essential for optimal functionality.

## 2. SYSTEM ARCHITECTURE



### 2.1 ARCHITECTURE WALKTHROUGH

#### 2.1.1 User Registration

- Individuals are directed to the website URL via the highly available Route53 DNS service. The website's homepage features a Sign-up/Sign-in page, enabling users to create an account using a valid email ID.
- Amazon Cognito simplifies the management of user groups by organizing users with common attributes, permissions, or roles within User Pools. This streamlines group-based access control and user administration.

#### 2.1.2 Data Input and Document Upload

- Users are required to complete a form with basic details such as Name, DOB, Address, Place of Birth, and upload a standard-size picture, along with an accepted identity document.

### 2.1.3 Document Processing: Text Extraction and Data Validation

- The user's uploaded identity document is stored in a preconfigured S3 bucket (Standard), later moved to Standard IA after 5 days for cost optimization.
- AWS Textract processes all uploaded files in batch mode every 12 hours, ensuring cost governance.
- AWS Lambda triggers the Textract process, verifying if the user-provided details match the document contents. Verified details are then updated in the RDS database.

### 2.1.4 User Notification and One-D Generation

- Users receive notifications of Success/Failure through AWS SNS.
- Users are issued a Unique ID (ONE-D), pending notarization.

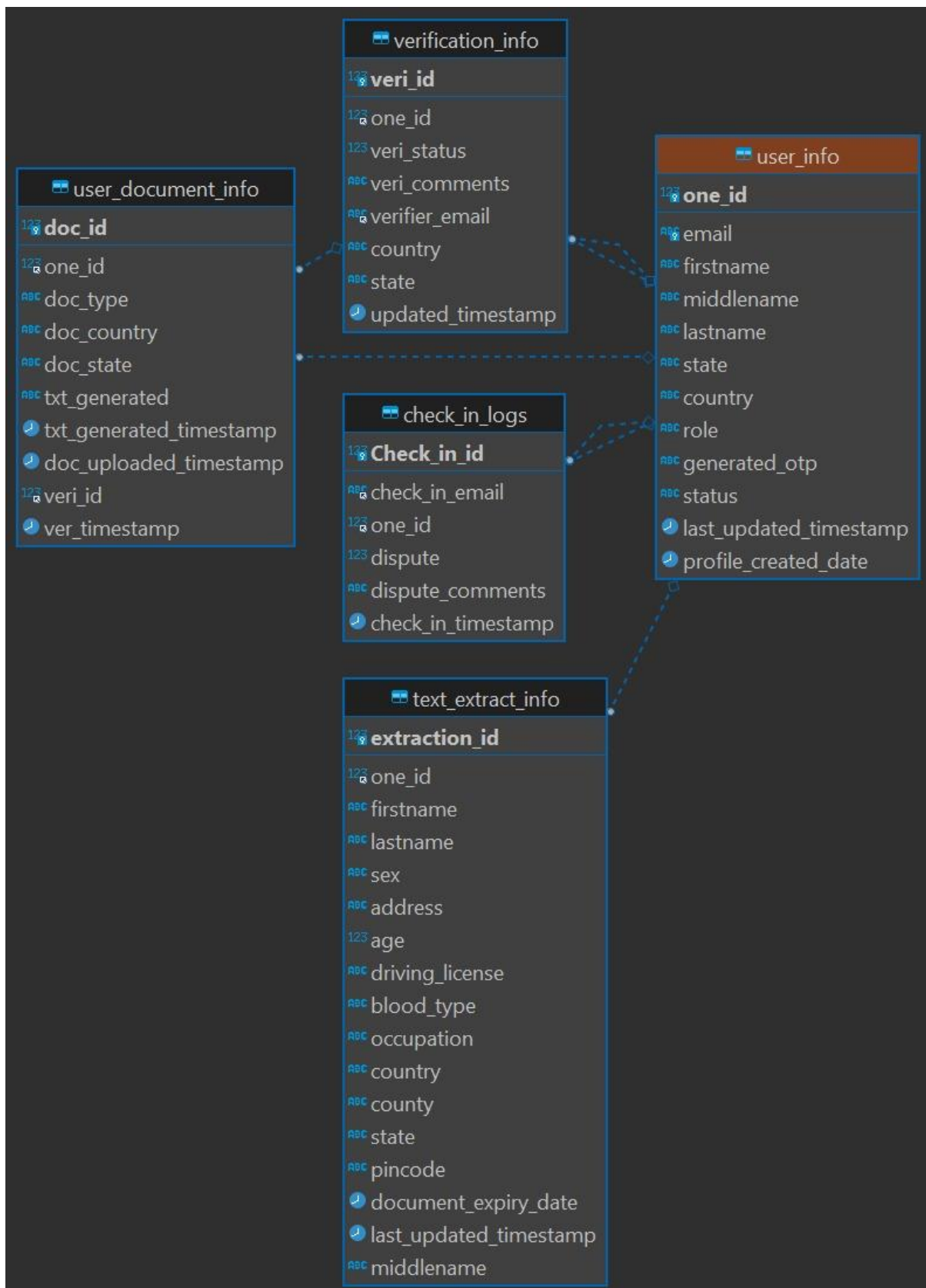
### 2.1.5 Notarization Process

- The user must physically appear at a partner notary organization (e.g., UPS).
- Notary officials sign in with pre-registered credentials, accessing an interface displaying user data and the uploaded identity document.
- RDS stores notarization success/failure based on the notary official's decision.

### 2.1.6 After Successful Notarization

- Third parties (hotels, pubs, etc.) sign in with pre-registered accounts. Upon entering the ONE-D of their client, non-confidential details are displayed for registration or age verification purposes.
- The notarized document serves as identity proof, replacing the need for physical documents, which are prone to forgery. The ONE-D authenticates individuals to third parties requiring identity proof.

## 2.2 ENTITY RELATIONSHIP DIAGRAM



## 3. USER MANUAL

### 3.1 For User:

#### 3.1.1 Initial registration

- Visit <https://www.one-d.cloud> .
- Select the User slider to sign-up.
- Enter the required fields and click “Submit” .
- Upload any one of the mentioned Government issued ID card in jpeg/pdf format.
- Note: The email and the phone number will be used for OTP purposes so make sure that you have access to these at all times.

#### 3.1.2 Confirming the details extracted from Identity Card

- Now in the next step, the text extracted from the ID card is displayed, you may edit this if needed. NOTE: The changes made will be final which will be audited by the notary body.

#### 3.1.3 In- Person Notarization Process

- During the in person notarization process, the notary official may ask you to confirm some details which you will be required to do so for the verification process to be successful.
- If the verification process is successful, you will receive a Success message at your registered email and phone.

#### 3.1.4 One-D Ready for Identity Proof!

- Now that your One-D is delivered to you, it is ready for use for 3<sup>rd</sup> party identity verification.
- At any 3<sup>rd</sup> party verification scenarios, provide them your unique One- D with the OTP and Voila! You do not need to carry your physical ID card to places you visit. Welcome to the Digital Era, now all you need is your One-D and your secure OTP to establish proof of identity



## 3.2 For Notary Official:

### 3.2.1 Initial Notary Sign Up:

- Visit <https://www.one-d.cloud> .
- Select the “Notary” option on the slider
- Enter the required fields and click “Submit”.
- Upload one of the mentioned Government issued ID card in jpeg/pdf format.
- Note: The email and the phone number will be used for OTP purposes so make sure that you have access to these at all times.
- Wait for account approval from One-D Administrator after which you may sign in for notarization purposes.

### 3.2.3 In- Person Notarization process

- Make sure that you are logged into your account
- Enter the One-D of the applicant who is present for the process
- Enter the OTP which is sent to the applicant on email/ text
- Now you will be redirected to the details page where each field will have 2 checkboxes, Correct and Incorrect.
- In the authority of the Notary Body, the notary official should verify the displayed fields after cross verification of the physical ID card. If there be any discrepancies, the field should be marked as incorrect.
- After going through all the fields, there will be a “Comments/ Raise Dispute” field where any additional comments may be added.
- Click on the “Submit” button to complete the process.

## 4. TECHNICAL DOCUMENTATION

### 4.1 Technologies Used

#### 4.1.1 Backend

- Flask: It is a great pick for One-D's backend, due to its simplicity and flexibility. It easily adapts to intricate tasks like identity management and notarization. With user-friendly features like dynamic routing and RESTful API support. This versatility ensures One-D smoothly handles user registration, document processing, and notarization. Flask's down-to-earth design makes it a sensible choice for building a dependable backend infrastructure for One-D's everyday processes.

Libraries used: boto3, json

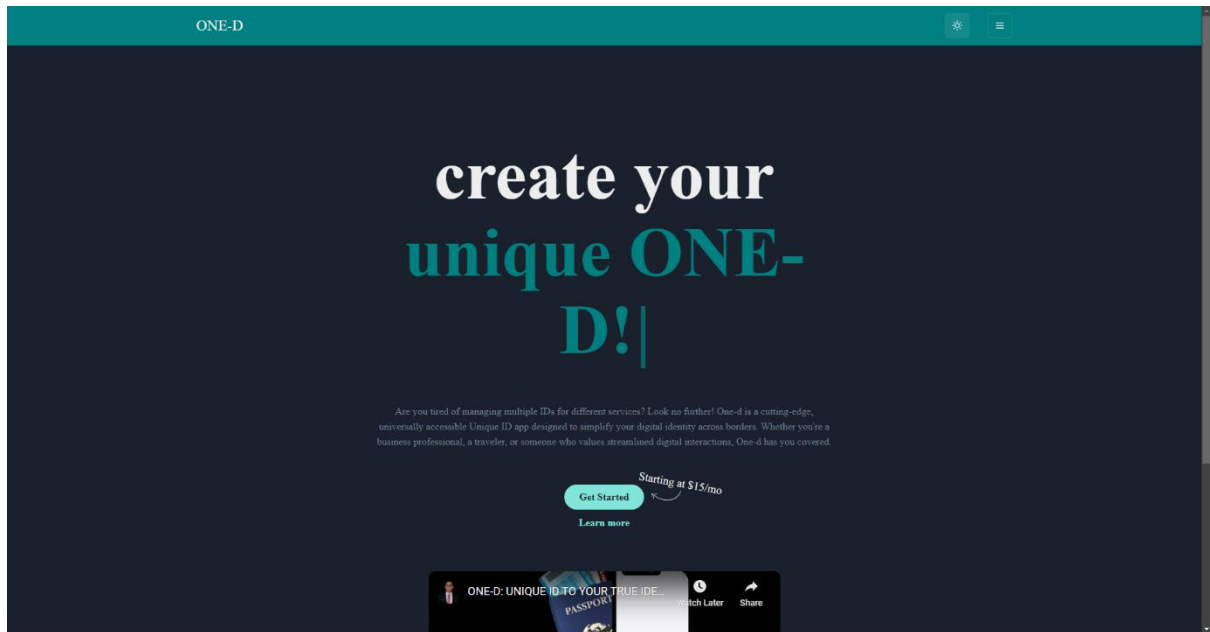
- MySQL server: Opting for MySQL as One-D's data storage solution proves pragmatic, combining reliability with simplicity. With its ease of use, MySQL seamlessly handles the storage needs of complex processes like identity management and notarization. Its robust features facilitate efficient data organization, retrieval, and scalability. Utilizing MySQL ensures One-D's ability to manage user information, process documents, and record notarization outcomes effectively. The straightforward design and widespread acceptance of MySQL make it a dependable choice for maintaining One-D's data.

#### 4.1.2 Frontend

- React: Choosing React as the frontend framework for One-D ensures a blend of efficiency and user-friendly design. React's declarative and component-based structure streamlines development, providing an effective solution for user interaction and document presentation in the One-D system. Its modular design fosters code organization and scalability. Implementing React guarantees a responsive and dynamic user interface, contributing to an enhanced overall user experience. React's widespread adoption and robust community support make it a pragmatic choice, aligning with One-D's thoughtful strategy for frontend development across various day-to-day applications. The UI is designed to establish trust with users such that they feel that their information is secure and safe, which One-D safeguards at all times.

## 4.2 Screenshots:

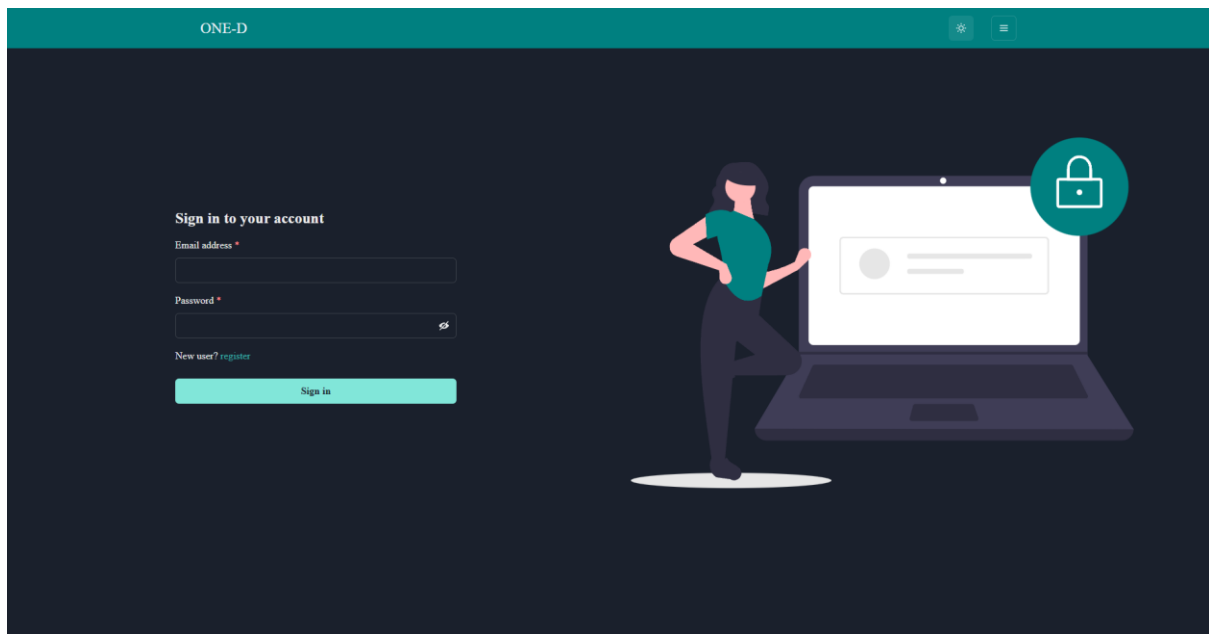
### 4.2.1 Homepage



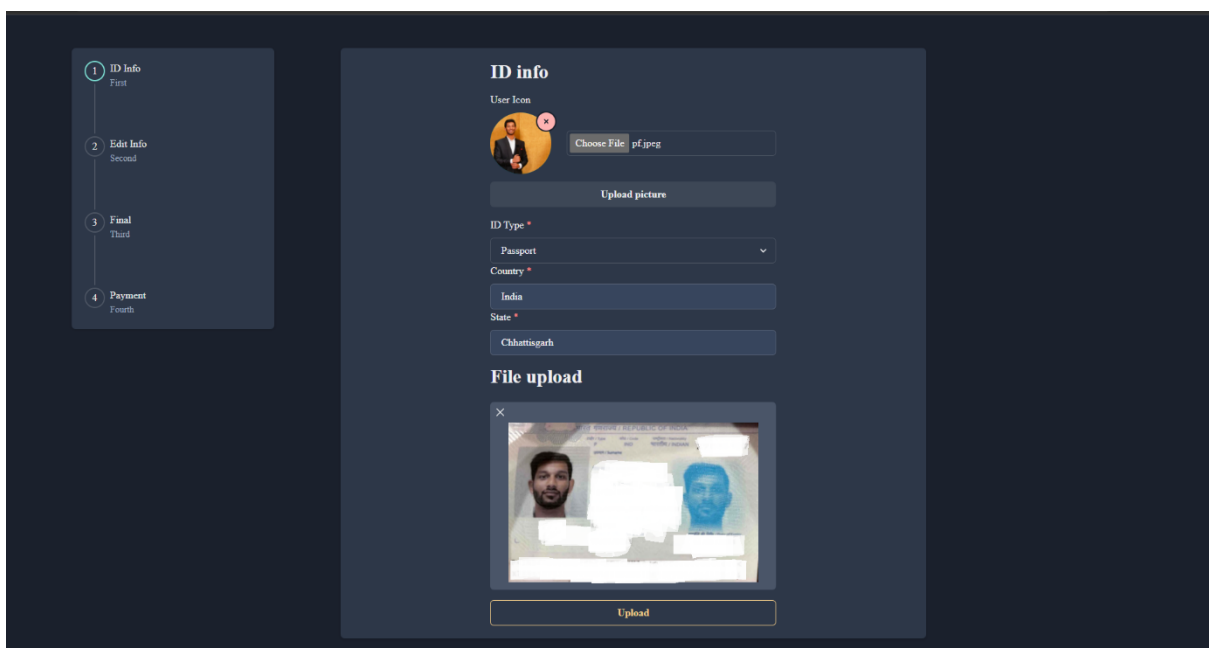
### 4.2.2 User Registration

The screenshot shows the user registration page of the ONE-D application. It features a teal header with "ONE-D" and navigation icons. The page is divided into two main sections. On the left, there is a "Create a new account" form with the following fields: "First Name \*", "Middle Name", "Last name \*", "Country \*", "State \*", "Email address \*", and "Password \*". Below the form is a link "Already a user? login" and a teal "Sign Up" button. On the right, there is a large illustration of a woman with dark hair, wearing a white long-sleeved shirt and dark pants, holding several teal document icons. She is surrounded by floating document icons and small white flowers at her feet.

### 4.2.3 User Sign In



### 4.2.4 Filling Personal Details



## 4.2.5 Final edit the info for database entry

ONE-D

Progress: 1. ID Info (First) 2. Edit Info (Second) 3. Final (Third) 4. Payment (Fourth)

### Edit info

First Name *	Middle Name	Last Name *
Gudamu Sai		Krishna

Document Type *	Document Number *
PASSPORT	

Country *	State *
India	Chhattisgarh

Country *	Pincode *
Durg	490006

Sex *	Occupation *
male	Student

Date of Birth(MM/DD/YYYY) *	Expiry(MM/DD/YYYY) *

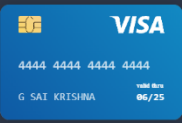
Address \*

Uploading

## 4.2.6 Payment

ONE-D

Progress: 1. ID Info (First) 2. Edit Info (Second) 3. Final (Third) 4. Payment (Fourth)



4444 4444 4444 4444  
G SAI KRISHNA  
valid thru 06/25

Card Number *	
4444444444444444	

Card Holder Name *	
G Sai Krishna	

Expiry *	CVC *
06/2025	CVC

Make payment

## 4.2.7 Notary Verification Page(For Notary User)

Notary

User Details

☒ Check all items

firstname

G Sai

☒

lastname

Krishna

☒

country

India

☒

state

Chhattisgarh

☒

Age

☒

Expiry

☒

Occupation

Student

Signature \*

Jeswanth Vadlamudi

Dispute

Approve

## 4.2.8 One-D Card

ONE-D

Receipt

Logs

Get OTP

34

Name: G Sai Krishna

Gender: Male

Age: 24

Expiry: 05/18/2033

Address

Lotus 67, Talpuri A Block, Bhilai

PASSPORT

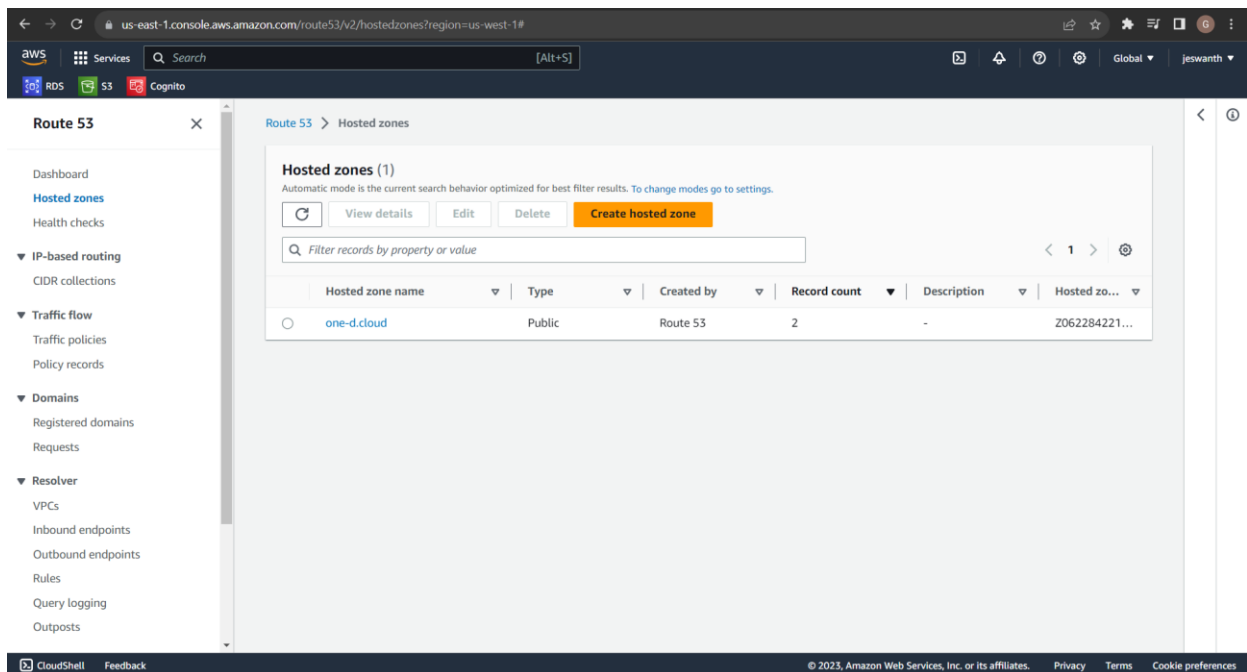
US

IN

14

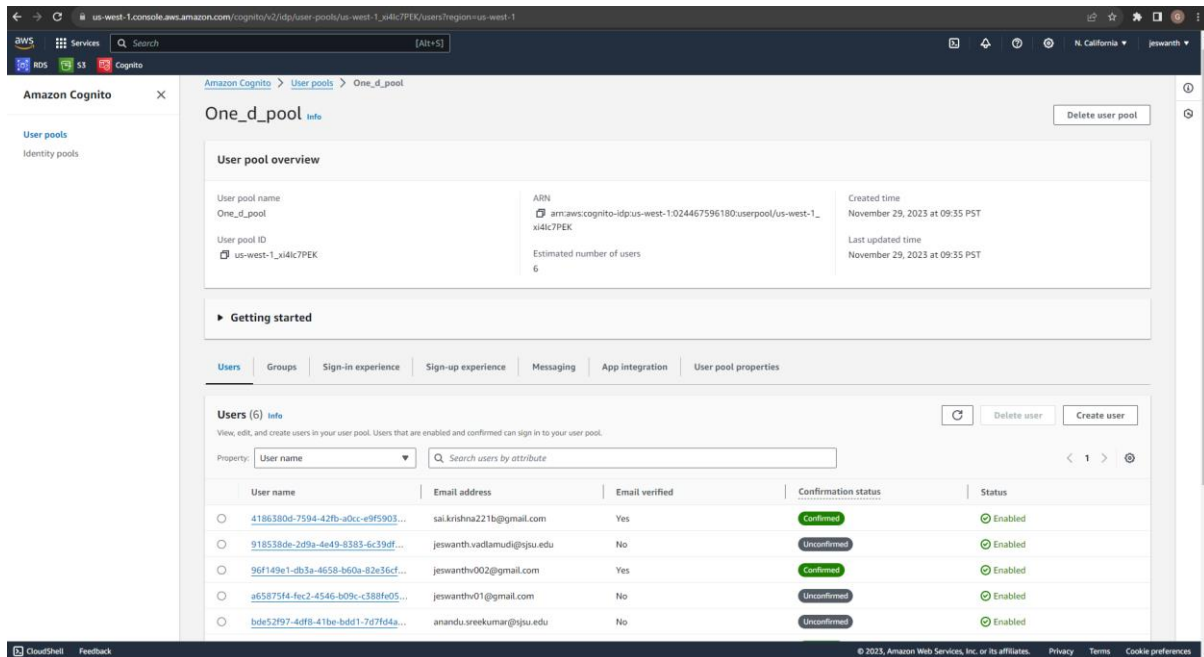
## 4.3 AWS Technologies Used:

**4.3.1 Route53:** Leveraging Route 53 for traffic management underscores our commitment to a robust, scalable, and efficient web infrastructure. As a highly available and scalable DNS service, Route 53 ensures reliable routing of user requests to our website. Its global network of authoritative DNS servers minimizes latency, optimizing the end-user experience across diverse geographic locations. Route 53 Load Balancers play an important role in distributing incoming traffic across multiple instances, promoting high availability and fault tolerance. With health checks and automatic failover mechanisms, Route 53 enhances the resilience of our web application, dynamically steering traffic away from unhealthy instances. Additionally, its integration with AWS services simplifies domain registration, DNS management, and enables quick adjustments to adapt to changing traffic patterns, making Route 53 a cornerstone in our strategy for a dependable and responsive web presence.

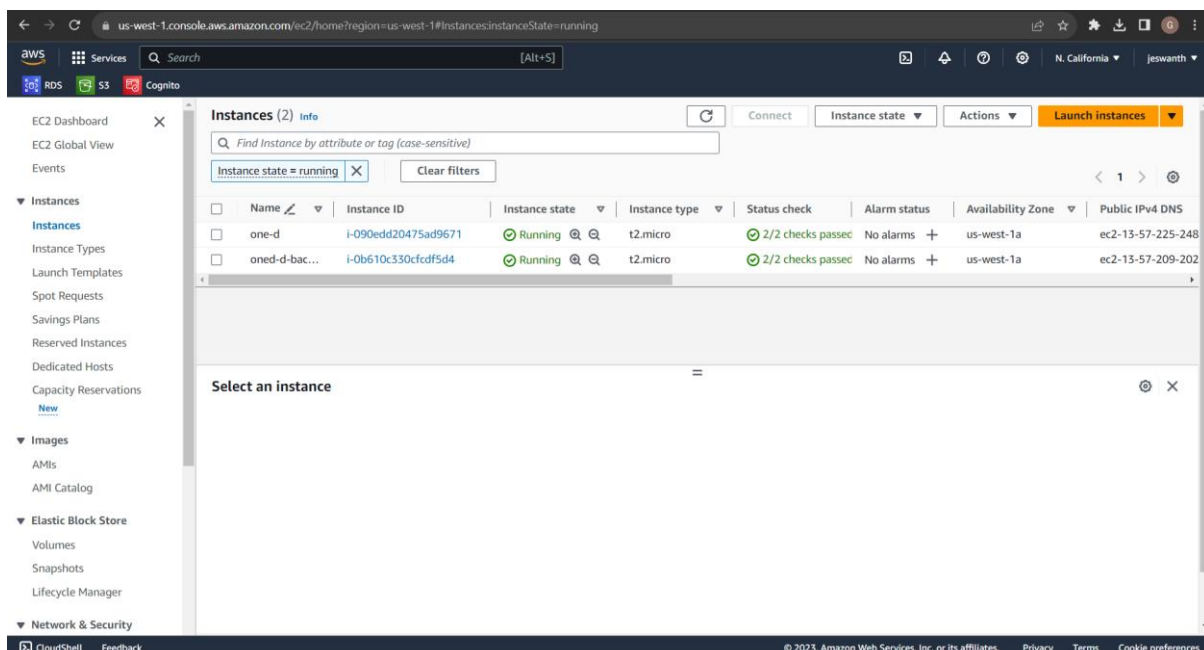


**4.3.2 AWS Cognito:** As a fully managed service, Cognito simplifies user authentication and authorization, significantly reducing the development effort needed for these critical components. Its versatile features enable easy integration with our web application, providing secure sign-up and sign-in functionality. Cognito's scalability aligns with our growth trajectory, efficiently handling user pools and identity management. With advanced security measures, such as multi-factor authentication, Cognito ensures a

robust shield against unauthorized access. Furthermore, its integration with other AWS services facilitates a cohesive and comprehensive solution, enhancing our ability to deliver a secure and user-friendly experience.

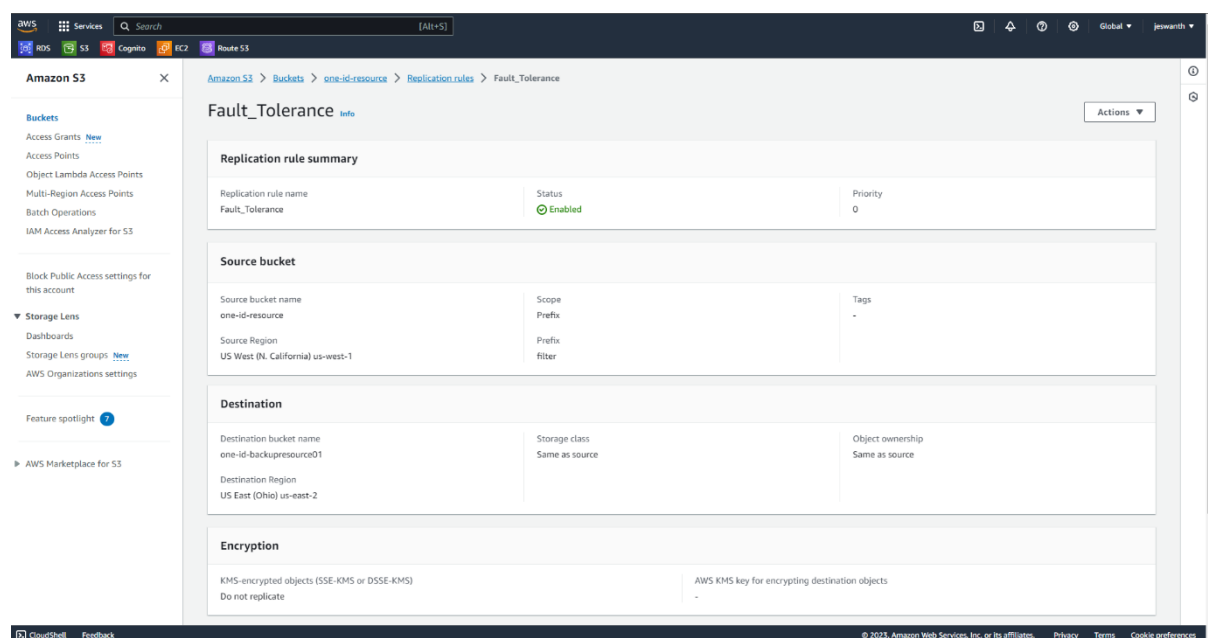


**4.3.3 AWS Elastic Compute Cloud (EC2):** For hosting the backend and frontend of One-D, EC2 serves as the cornerstone of our infrastructure. Leveraging EC2 instances, we ensure the scalability, flexibility, and reliability required for a seamless UX. The backend, powered by Flask, is deployed on an EC2 instance, offering a robust and scalable environment for handling user registrations, document processing, and notarization. Simultaneously, the React frontend is hosted on an EC2 instance, providing users with a responsive and dynamic interface. The versatility of EC2 enables efficient resource allocation, ensuring optimal performance even during peak loads.





4.3.4 **AWS S3:** as our primary storage solution for user-uploaded files is fundamental to our data management strategy. By relying on the industry-grade encryption provided by S3, we prioritize the security and confidentiality of user data, ensuring its protection throughout its lifecycle within our system. The integration of our Lambda function with S3 files enhances the efficiency of processing and managing these uploads. Furthermore, we've implemented lifecycle policies within S3 to optimize cost savings, ensuring that data transitions appropriately between storage classes based on usage patterns. S3's scalability, durability, and cost-effective features align with our growing data requirements, guaranteeing a safe, scalable, and economically efficient storage solution. This approach reinforces our commitment to data integrity, user privacy, and operational efficiency. Attached is the Replication Rule for one s3 bucket to another for **Multi AZ Support**. A lifecycle policy is enabled for cost optimization.



4.3.5 **AWS Textract:** Harnessing the power of AWS Textract for extracting information from user-uploaded ID cards represents the extent to which this project endeavors to include new technology. By integrating machine learning (ML) trained functions into the text extraction process, we elevate the efficiency and accuracy of information retrieval. Textract's advanced ML models intelligently analyze and comprehend diverse document structures, ensuring precise extraction of relevant details from ID cards. This sophisticated integration not only streamlines the user experience but also enhances the overall reliability and speed of our identity verification processes. Note: Textract is invoked using Lambda.

The screenshot shows the AWS Lambda console interface. The top navigation bar includes the AWS logo, a search bar, and service icons for RDS, S3, and Cognito. The main content area is titled 'Code source' and displays the Python code for a Lambda function. The code is as follows:

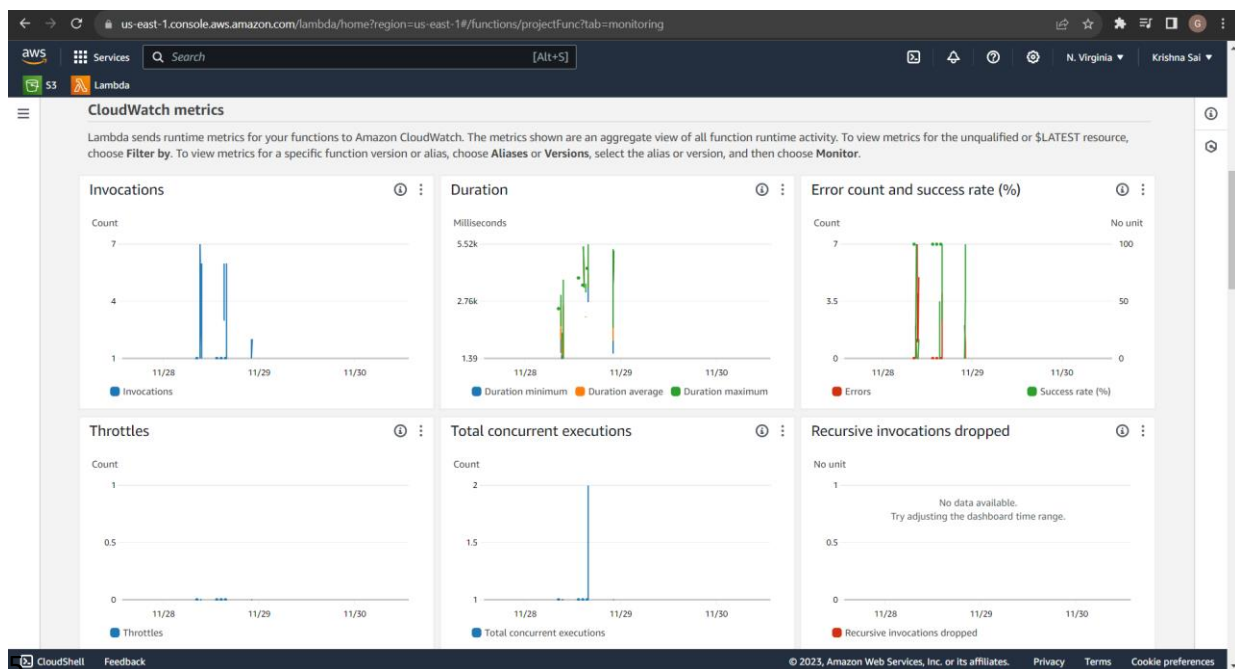
```
1 import json
2
3 def lambda_handler(event, context):
4
5     payload = json.loads(event['body'])
6     object_key = payload.get('key', None)
7
8     textract_client = boto3.client('textract')
9
10    # Call the analyze_document API
11    response = textract_client.analyze_id(
12        DocumentPages=[{'S3Object': {'Bucket': 'one-id-resource', 'Name': object_key}}]
13    )
14    dic = {}
15
16    # Extract the text from the response
17    extracted_text = ''
18    for doc_fields in response['IdentityDocuments']:
19        for id_field in doc_fields['IdentityDocumentFields']:
20            for key, val in id_field.items():
21                if "Type" in str(key):
22                    x = val['Text']
23                for key, val in id_field.items():
24                    if "ValueDetection" in str(key):
25                        dic[x] = val['Text']
26
27    # Convert data to JSON string
28    json_data = json.dumps(dic)
29
30    return {
31        'statusCode': 200,
32        'body': json_data
33    }
```

4.3.6 **AWS RDS: Employing AWS RDS as the bedrock for deploying our MySQL database** signifies a strategic choice for ensuring a robust and scalable data management infrastructure. RDS streamlines database administration tasks, allowing us to focus on optimizing reads and writes without the overhead of routine maintenance. The centralized MySQL database, hosted on RDS, serves as a central hub for all data interactions. With automated backups, security protocols, and scalability options, RDS not only enhances data integrity but also facilitates seamless scaling to accommodate growing demands. This strategic implementation aligns with our commitment to a secure, efficient, and scalable database solution, empowering us to deliver a responsive experience for our users.

The screenshot shows the AWS RDS console interface. The top navigation bar includes the AWS logo, a search bar, and service icons for RDS, S3, and Cognito. The main content area is titled 'Databases (2)' and displays a table of databases. The table has the following columns: DB identifier, Status, Role, Engine, Region & AZ, Size, Actions, CPU, Current activity, and Maintenance. The data is as follows:

DB identifier	Status	Role	Engine	Region & AZ	Size	Actions	CPU	Current activity	Maintenance
databaseoned	Available	Instance	MySQL Community	us-west-1b	db.t3.micro	3 Actions	3.51%	2 Connections	none
filango	Stopped temporarily	Instance	MySQL Community	us-west-1a	db.t3.micro	-	-	-	none

**4.3.7 AWS CloudWatch:** Utilizing AWS CloudWatch provides a comprehensive overview of Lambda function calls, crucial for monitoring and optimizing system performance. CloudWatch offers real-time insights into execution metrics, enabling proactive issue identification. This transparency ensures system efficiency and responsiveness, with alarms for automated notifications on performance thresholds. CloudWatch streamlines monitoring, reinforcing our commitment to a high-performance, resilient system.



**4.3.8 AWS Lambda:** In the architecture of our application, AWS Lambda plays a crucial role in integrating Textract with our Flask backend. When a user uploads an ID card through our application, the Flask backend triggers a Lambda function, specifically designed to invoke the Textract analyzeID function. This Lambda function acts as a bridge between the front-end and the powerful text extraction capabilities of Textract. As the uploaded ID card is processed, Lambda efficiently analyzes the document, extracting relevant textual information. The orchestrated collaboration between Flask, Lambda, and Textract underscores our commitment to an efficient, modular, and cloud-native architecture, facilitating the extraction of text from uploaded ID cards for a user experience worth remembering.

Amazon Web Services (AWS) console interface showing the configuration for the **ExtractDocumentText** Lambda function.

**Function overview**

- Diagram** / Template
- Function name: **ExtractDocumentText**
- Layers: (0)
- + Add trigger
- + Add destination
- Buttons: Throttle, Copy ARN, Actions, Export to Application Composer, Download function
- Metadata:
  - Description: -
  - Last modified: 5 days ago
  - Function ARN: `arn:aws:lambda:us-west-1:024467596180:function:ExtractDocumentText`
  - Function URL: [info](#)

**Configuration** (selected tab)

- General configuration
- Triggers
- Permissions** (selected)
- Destinations
- Function URL
- Environment variables
- Tags

**Execution role**

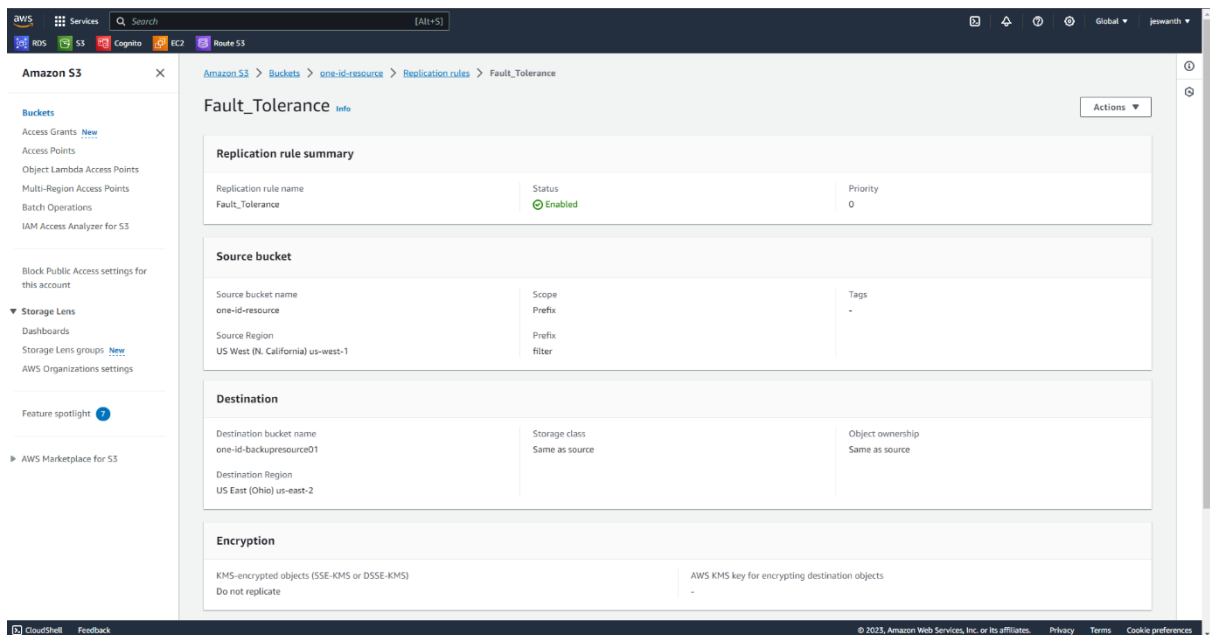
- Role name: [LambdaUSER](#)
- Buttons: Refresh, Edit, View role document
- Resource summary**
- To view the resources and actions that your function has permission to access, choose a service.
- Selected resource: **Amazon CloudWatch Logs** (5 actions, 2 resources)

Footer: © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

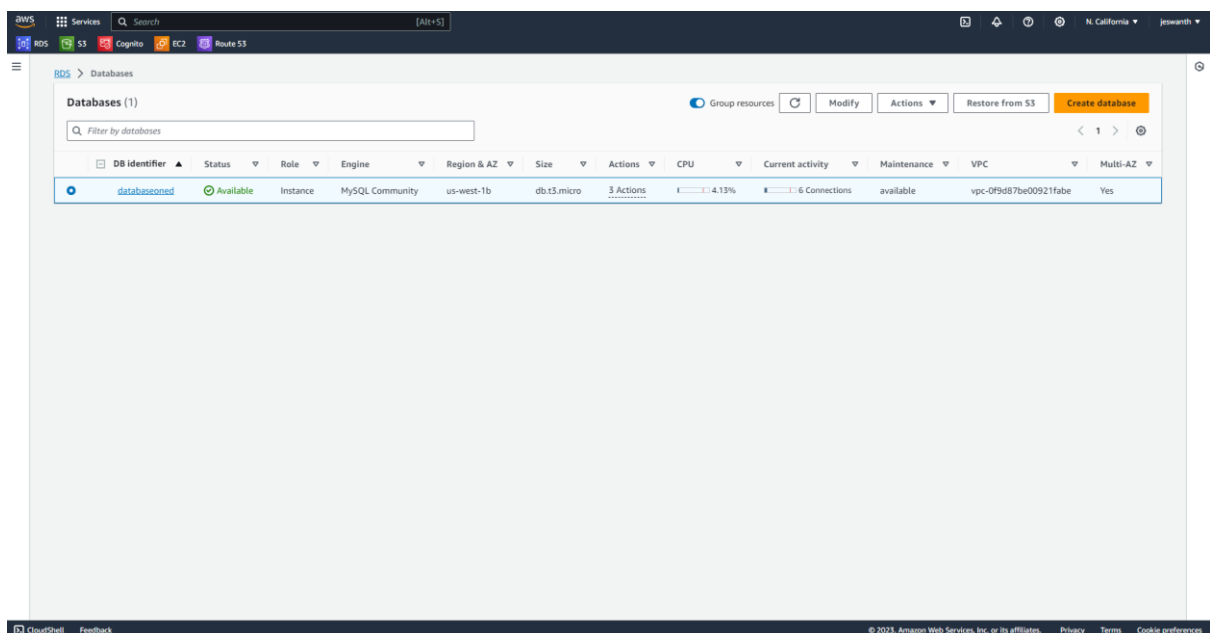
## 4.4 Cloud Best Practices

### 4.4.1 High Availability and Disaster Recovery achieved through Multi AZ support in S3 and in RDS.

Multi AZ Replication rule for a backup bucket in AWS S3:

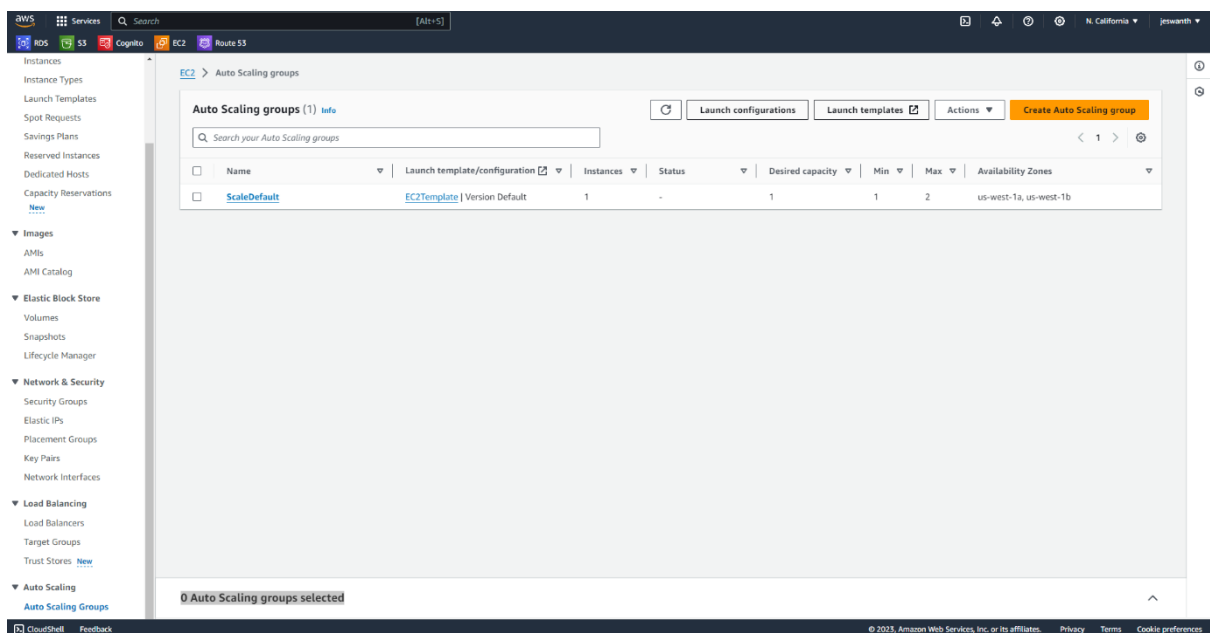
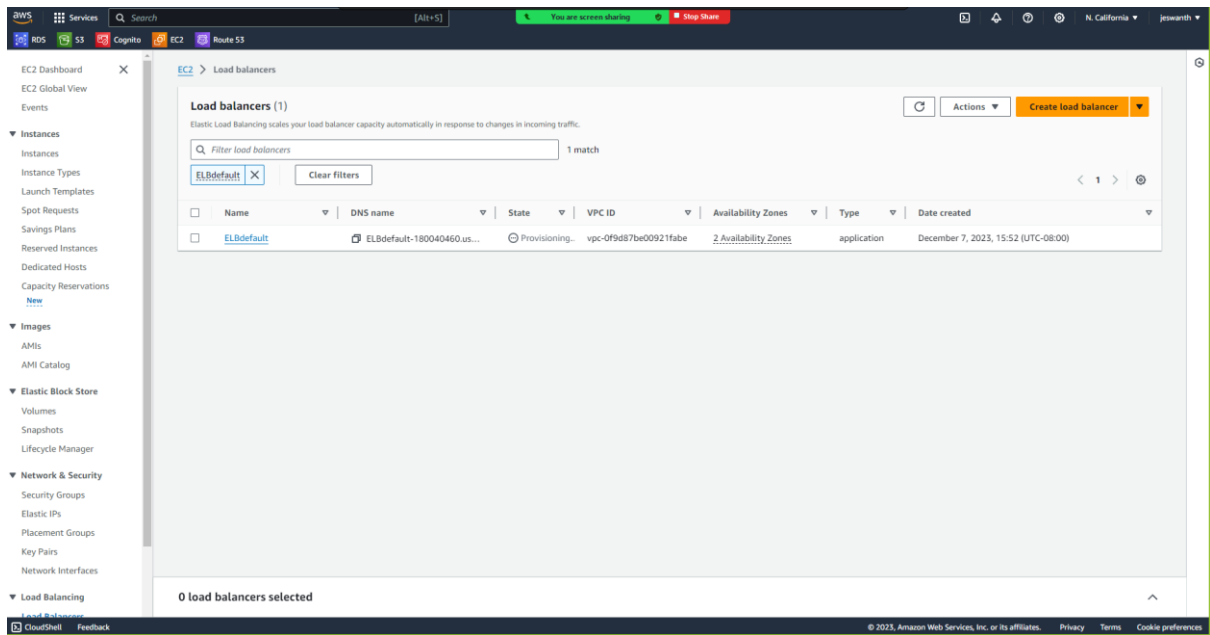


Multi AZ Support for RDS enabled:



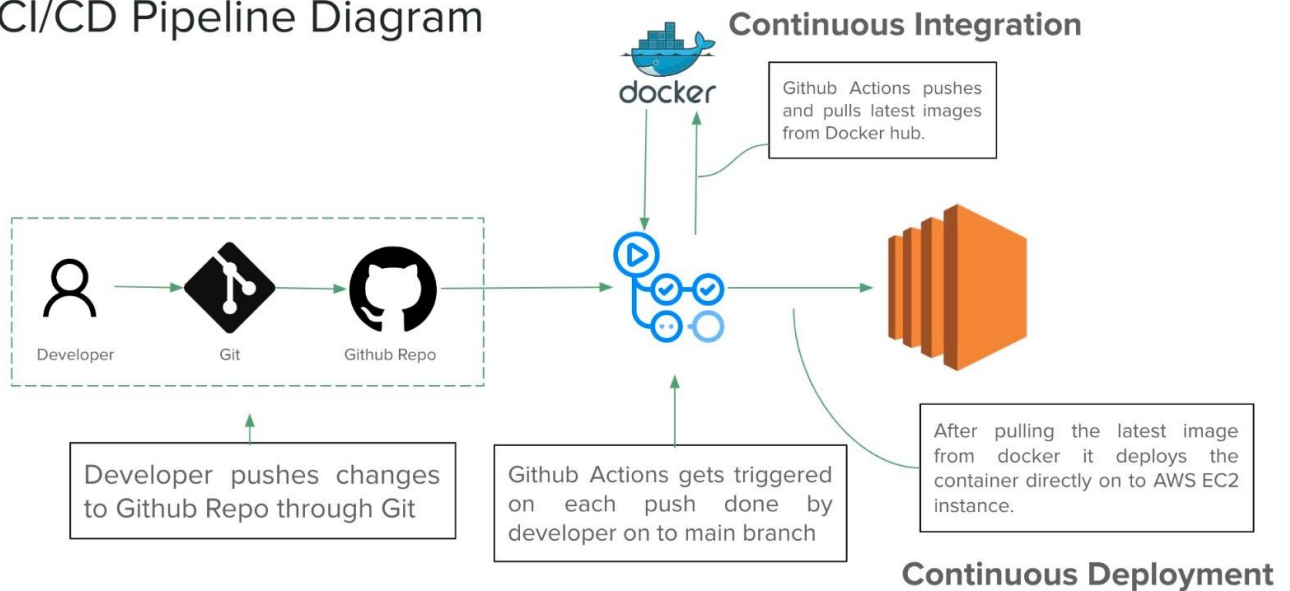
## 4.4.2 Fault Tolerance:

Elastic Load balancer and AutoScaling group created



## 4.5 CI/ CD Pipeline

### CI/CD Pipeline Diagram

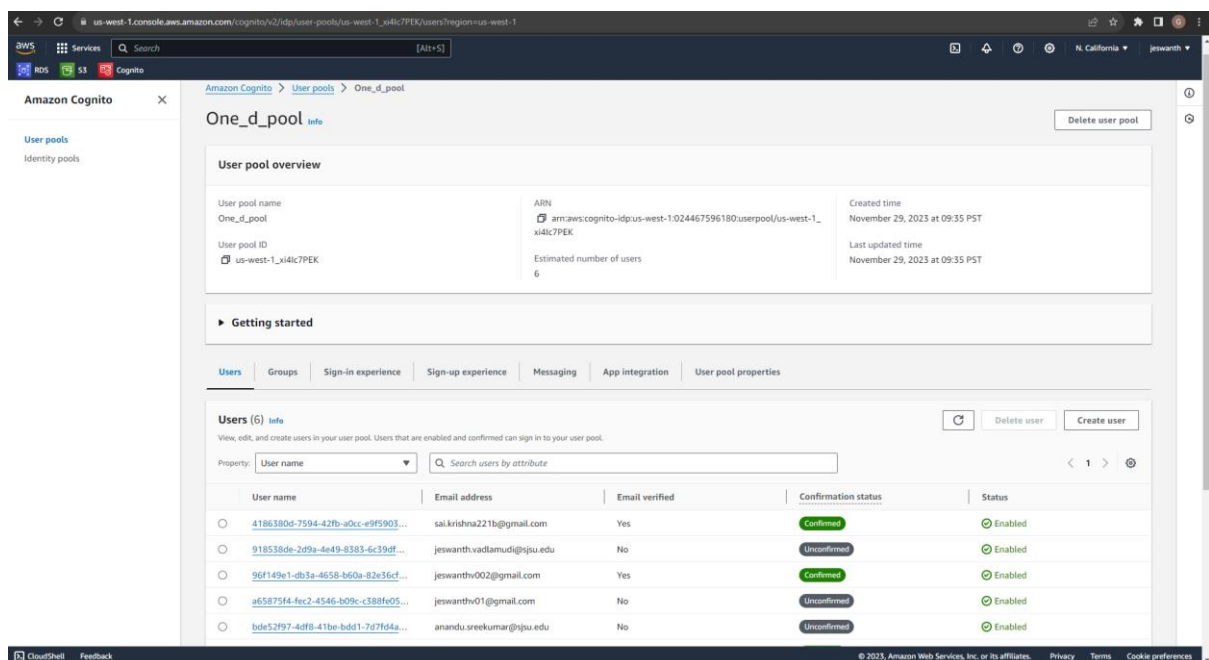


Every push made by a user triggers actions that automatically push and download Docker images from Docker Hub by using GitHub, Git, and GitHub Actions. By ensuring that the most recent image is deployed into an EC2 instance, the automated process improves dependability and efficiency. This coordinated procedure offers a solid method for safe digital ID verification by combining version control, containerisation, and continuous deployment. Our deployment pipeline's collaborative and automated design guarantees timely and dependable upgrades, bolstering the authentication system's overall integrity.

## 5. SECURITY MEASURES:

### 5.1 Authentication and Authorization Mechanisms

Using AWS Cognito for user login and authentication reinforces our application's resilience against potential data breaches. Cognito employs advanced encryption protocols during the authentication process, ensuring the confidentiality of user credentials and shielding them from unauthorized access. The implementation of Multi-Factor Authentication (MFA) provides an additional layer of security, requiring extra verification steps even if login credentials are compromised. Cognito's adept management of user directories and identity pools establishes a secure environment for storing and handling user profiles, incorporating encryption at rest to safeguard user data. The service's ongoing monitoring and automated threat detection further heighten its defenses against a spectrum of cyber threats, making Cognito an integral and reliable solution for robust and secure user authentication.



The screenshot displays the Amazon Cognito console interface. The top navigation bar shows the AWS logo, a search bar, and the user's profile. The left sidebar contains the 'Amazon Cognito' logo and a menu with 'User pools' and 'Identity pools'. The main content area is titled 'One\_d\_pool' and includes a 'Delete user pool' button. Below this is a 'User pool overview' section with details such as the user pool name, ARN, user pool ID, and estimated number of users. A 'Getting started' section is also present. The 'Users' tab is selected, showing a list of 6 users. The table includes columns for User name, Email address, Email verified, Confirmation status, and Status. The users are listed with their respective email addresses and confirmation statuses.

User name	Email address	Email verified	Confirmation status	Status
4186380d-7594-427b-a0cc-e9f5903...	sai.krishna221b@gmail.com	Yes	Confirmed	Enabled
918538de-2d9a-4e49-8383-6c39df...	jeswanth.vadlamudi@sjpu.edu	No	Unconfirmed	Enabled
96f149e1-db3a-4658-b60a-82e36cf...	jeswanth002@gmail.com	Yes	Confirmed	Enabled
a65875f4-fec2-4546-b09c-c388fe05...	jeswanth01@gmail.com	No	Unconfirmed	Enabled
bde52f97-4df8-41be-bd01-7d7f64a...	anandu.sreekumar@sjpu.edu	No	Unconfirmed	Enabled



## 5.2 Handling and Storage of Sensitive Information

Storing user-uploaded identity cards in AWS S3, fortified by server-side encryption, forms a robust security shield against potential data breaches. The server-side encryption mechanism ensures that data is encrypted before it is written to disk, rendering it unreadable without the corresponding decryption key. This stringent encryption protocol significantly reduces the risk of unauthorized access and safeguards sensitive user information from potential breaches. AWS S3's encryption-at-rest feature provides an additional layer of protection, bolstering the overall security posture. By adopting server-side encryption within S3, we prioritize the confidentiality and integrity of user data, fortifying our commitment to a secure and resilient environment that withstands the evolving landscape of potential threats and cyber vulnerabilities.

## 6. VERIFICATION PROCESS:

The Notarization process within One-D is a meticulous and secure procedure that involves distinct steps with stringent guidelines to ensure the authenticity of user identity. For users, the journey initiates with the initial registration on the One-D platform, accessible at <https://www.one-d.cloud>. After providing essential details and uploading a government-issued ID card in jpeg/pdf format, users confirm the extracted information displayed on the platform. This step is critical, as any edits made will be finalized and audited by the notary body. The subsequent in-person notarization process involves confirming details with the notary official, leading to a success message upon successful verification.

Notary officials undergo a specific onboarding process by selecting the "Notary" option on the platform slider and submitting requisite details along with a government-issued ID card. After account approval by the One-D Administrator, notary officials can sign in for notarization purposes. During the in-person notarization, officials verify the One-D of the applicant, enter the OTP sent to the applicant, and proceed to cross-verify displayed fields with the physical ID card. The official marks each field as correct or incorrect, providing additional comments if necessary. The meticulousness of this process ensures the accuracy and reliability of the information stored within the One-D system. Upon completion, users receive a One-D that serves as a digital identity proof for third-party verifications, marking a transition into the digital era, where a single One-D and OTP suffice for establishing identity without the need for physical ID cards. This innovative approach streamlines identity verification while maintaining security and compliance.

### Establishing Identity Proof with Third Party- After Successful Notarization Process:

Establishing identity proof with third parties through the seamless integration of One-D and OTP is a remarkably efficient and secure process that encapsulates the progressive modernization of identity verification. Users wielding their unique One-D can navigate third-party verification scenarios with remarkable ease. This simplicity is underscored by the straightforward act of presenting the One-D alongside the OTP received on their registered email or phone, completely eliminating the need for cumbersome physical ID cards. This transformative approach marks a substantial shift toward a digital era, where the conventional reliance on traditional documents gracefully yields to a seamless and technologically advanced method.

The One-D, complemented by the OTP, forms a robust and dynamic duo, offering users not only unparalleled convenience but also significantly elevating security standards in the validation of their identity for third-party interactions. This contemporary methodology not

only enhances the user experience but also aligns with the broader trajectory of digitization and innovation within identity verification processes. This fusion of user-friendly accessibility and heightened security positions the One-D and OTP tandem as a pioneering solution, shaping a future where identity authentication seamlessly integrates into the digital fabric of everyday interactions. The ongoing evolution of identity proof, spurred by advancements like One-D and OTP, symbolizes a paradigm shift, heralding an era where the simplicity of digital interactions converges with the robustness of security measures, setting new standards for the authenticity and efficiency of identity verification in our increasingly interconnected world.

## 7 SCALABILITY AND FUTURE IMPROVEMENTS

### 7.1 Enhanced User Capacity:

To fortify One-D's infrastructure for scalability, prioritizing enhanced user capacity is paramount. This involves implementing robust load balancing mechanisms and optimizing database management systems. By doing so, One-D ensures the platform's ability to seamlessly accommodate a burgeoning user base without compromising operational performance.

The scalability roadmap for One-D incorporates a strategic focus on global accessibility. The project envisions expanding its reach to users worldwide, accounting for diverse regional compliance requirements and user preferences. A scalable solution must be adaptable to different jurisdictions, ensuring One-D's inclusivity and relevance on a global scale.

In the pursuit of scalability, One-D recognizes the significance of continual user experience refinement. Regular solicitation of user feedback and subsequent implementation of user-friendly upgrades are integral components of this strategy. This encompasses streamlining the registration process, optimizing the user interface, and introducing features aligned with evolving user expectations. These efforts are designed to foster heightened user engagement and satisfaction, contributing to One-D's sustained scalability.

### 7.2 Advanced Verification Mechanisms:

As part of ongoing enhancements, One-D aims to augment the platform's security and reliability through the exploration and integration of advanced verification mechanisms. Moving beyond traditional notarization, the project will investigate cutting-edge technologies such as biometric authentication and blockchain-based verification. These innovations are poised to elevate the overall trustworthiness of One-D's identity verification processes.

## 8 CONCLUSION:

### 8.1 Summary of the Project

The One-D project stands as a pioneering endeavor that will, we expect reshaped the landscape of identity verification, introducing a paradigm shift in the way users authenticate their identities. At its core, the project achieved a seamless and secure user registration process, leveraging cutting-edge notarization protocols to establish a robust digital identity solution. The platform effectively eliminates the dependence on traditional physical ID cards, offering users a technologically advanced alternative.

Through meticulous planning and execution, the project successfully addressed the intricate challenges associated with identity verification, providing a scalable and adaptable solution. The user-centric approach adopted throughout the project's lifecycle ensures that One-D not only meets but exceeds user expectations. The platform's transformative impact extends beyond its functional attributes, contributing to a broader narrative of digitization and innovation in identity management. As we reflect on the summary of the project, it becomes evident that One-D has not merely created a digital identity solution; it has laid the foundation for a new era in secure, efficient, and user-centric identity verification.

Cloud best practices have been followed in this project to facilitate High Availability, Fault Tolerance achieved through MultiAZ deployment and Replication Rules. Cost Optimization has been achieved through S3 bucket lifecycle policy.

### 8.2 Lessons Learned

Throughout the project's lifecycle, valuable lessons have been garnered. The dynamic nature of identity verification underscored the necessity for continual adaptation, prompting the exploration and integration of innovative technologies such as biometric authentication and blockchain for advanced verification mechanisms. The significance of global accessibility became evident, leading to strategic considerations for diverse compliance requirements and user demographics. These lessons serve as a foundation for informed decision-making in future projects.

## 9 REFERENCES

- Flask Documentation: The official documentation provides comprehensive information on Flask, including installation, routing, templates, and more.
- Flask Mega-Tutorial by Miguel Grinberg
- React Documentation: The official documentation is a great starting point for learning React, covering concepts like components, state, and props.
- React - A JavaScript library for building user interfaces: The official React tutorial guides you through building a tic-tac-toe game, providing hands-on experience.
- MDN Web Docs - React: Mozilla Developer Network offers a comprehensive guide to getting started with React.
- AWS Documentation: The official AWS documentation is a treasure trove of information on all AWS services. Explore specific services like Lambda, S3, Cognito, Textract, RDS, and more
- AWS Lambda Documentation: Learn about AWS Lambda, a serverless compute service, and understand how to execute code without provisioning or managing servers.
- Amazon S3 Documentation: Dive into Amazon Simple Storage Service (S3) documentation to understand object storage in the cloud.
- Amazon Cognito Documentation: Explore Amazon Cognito documentation for user identity and access management in the AWS Cloud
- AWS Textract Documentation: Learn about AWS Textract, a fully managed machine learning service that automatically extracts textual content, forms, and tables from scanned documents
- Amazon RDS Documentation: Understand Amazon Relational Database Service (RDS) documentation for managing relational databases in the cloud

Code Repository Link: <https://github.com/AnanduSreekumar/ONE-D>

## 10 Individual Contributions

User	Type	Features	Framework
Anandu Sreekumar	Front-End	Notary Validation portal, Check-in validation Portal - Authentication, Login	React
	Back-end	log-in,Signup,upload, Questionare generation, one-d pass,stage update, user able creatio	Flask
	AWS	RDS,S3,EC2 backend, Cloudwatch, Route 53 and Domain setup	
	Research	AWS Textract potential	
	Documentation	Architecture Diagram and Introduction	
Jeswanth Vadlamudi	Front-End	User Potal - Sign-in,Upload, Check-in validation Log-in , Application progress	React
	Back-end	Validation check for notary system, Auditing, Edit information	Flask
	AWS	IAM, Textract, EC2 Frontend, Cognito	
	Research	Future aspects and Encryption of Data	
	Documentation	Component divition and Costs	
Sai Krishna	Front-End	Admin page - control and login, One-ID virtual card	React
	Back-end	Textract Lambda integration, One-ID generation, Admin user control, Auditing table	Flask
	AWS	SNS Topics, Lambda,Security, Autoscaling and load balancer	
	Research	Amazon Rekognition possible use case with the project	
	Documentation	Architecture Explanation and Future aspects	

## 11 Test User Credentials:

User: jeswanthv001@gmail.com

password: jeswanth@99

Notary : anandu.sreekumar@sjsu.edu

password: Anandu@99

Checker: jeswanthv002@gmail.com

Password:jeswanth@99

Administrator username: gudumusaikrishna@sjsu.edu

Password: Krishna@99

## 12 AWS Costs

