MINOR-2 PROJECT

SYNOPSIS MID-TERM REPORT

For

Multi Factor Authentication Using Facial Recognition

Submitted By

Specialization	SAP ID	Name
CCVT(Hons.)	500083761	Pranav Malik
CCVT(Hons.)	500087901	Divyansha Jeengar

Department of Systemics

School Of Computer Science

UNIVERSITY OF PETROLEUM & ENERGY STUDIES,

DEHRADUN- 248007. Uttarakhand

Project Guide **Cluster Head**

School of Computer Science
University of Petroleum & Energy Studies, Dehradun

Mid-term Report

1. Project Title

Multi Factor Authentication Using Facial Recognition

2. Abstract

Multifactor authentication is an essential tool in booming technology era to ensure the security of physical and virtual resources. Facial recogniton is one of the method that is popularly used for authentication these days. It is a biometric technology that is used in this project as a multifactor authenticator to authenticate the user while accessing a web application.

Multi factor authentication adds up an security layer to resources which ensures that only the authenticated user can get access to resources provided. As the login credentials can be stolen or leaked by any individual. Multifactor authentication reduces the chances of online resources being exposed to unauthenticated person.

This project uses various Cloud services provided by AWS such as Rekognition, S3 Bucket, AWS Lambda, Cognito to build multifactor authentication mechanism that uses the facial recognition as a secondary authentication tool after the login authentication process.

Hence, whenever a legitimate user tries to use the web application, they first need to login using their corresponding email addresses and then they will be again authenticated using their facial input using the previously stored data of their face in a database.

3. Introduction

in the digital age where all the data and sensitive information is being stored online, it is very important to ensure that the reight and authenticated user is geting access to the sensitive data. Traditional password based authentication has a lot of drawbacks and vulnerabilities associated with it. As it is vulnerable to haccking, phishing an identity threat. Which lead to an additional layer of security after the traditional password method. This multifactor authentication technique is an effective solution this problem.
Multifactor Authenticaion is used to ensure that the authenticated person is accessing and using the resources. thai security measure requires more the one from of identification before providing access to any resource.
As the technology is growing faster everyday, its user and intruders are also growing rapidly. These intruder can potentially damage or misuse the online resources of any organization or individual. In such scenerios multifactor authentication adds ups an extra layer of security to resources that ensures that only authenticated user gets the access to the resources.

Facial recognition technology (FRT) is a biometric technology that uses unique facial features to identify individuals. It analyzes the unique contours and features of a person's face, such as the distance between the eyes and the shape of the jawline.
In this project the AWS Rekognition is used to create a group of abled users that are used to recognise the authenticated users.

AWS Rekognition

AWS Recognition is a cloud based sefrvice of AWS that help developer to get image and video analysis easily without and requiring machine learning expertise. AWS Recognition in an image recognition project. We focus on how AWS Recognition can be used to improve the accuracy and efficiency of image recognition algorithms by leveraging its pre-trained models and APIs.
We first provide an overview of image recognition technology and its applications, highlighting the challenges associated with building and deploying image recognition systems. We then introduce AWS Recognition and its key features, including its pre-trained models for object and scene detection, facial analysis, and text detection. We also provide a review of the existing literature on AWS Recognition and its use in image recognition projects.

Next, we present a case study of an image recognition project that utilizes AWS Recognition. We describe the project's architecture, which includes an AWS Lambda function that processes images and videos using AWS Recognition APIs. We provide a detailed analysis of the performance and accuracy of the AWS Recognition models and compare them to other image recognition solutions.

AWS rekognitio used a large number of labels that are beings used to later recognise a face or an object. AWS recognition uses DetectLabels API to identify the dominant features of any stored or captured image. AWs Rekognition uses StartLabelDetection to detect the label in already stored videos and CreateStreamProcess to detect labels in Streaming video.

AWS Lambda Function

Image recognition is a powerful technology that has revolutionized the way we interact with visual data. One of the key challenges in image recognition projects is the processing power required to analyze large amounts of image data in real-time. This is where serverless computing comes in, offering a cost-effective and scalable solution to this challenge. AWS Lambda is a popular serverless platform that enables developers to build and run applications without the need for dedicated servers or infrastructure.Lambda functions can be used to improve the speed and efficiency of image processing by providing a scalable and cost-effective platform for running image recognition algorithms.

AWS Lambda functions in image recognition projects, including the benefits and limitations of this approach. We conclude that AWS Lambda provides a powerful and cost-effective solution for image recognition projects, enabling developers to process large amounts of image data in real-time without the need for dedicated servers or infrastructure. By leveraging the power of serverless computing, image recognition projects can become more efficient,

scalable, and cost-effective, paving the way for new applications in fields such as healthcare, security, and entertainment.

Amazon Cognito

AWS Cognito is a powerful user authentication and identity management service that enables developers to easily add user sign-up, sign-in, and access control to their applications. In an image recognition project, AWS Cognito can be used to authenticate and manage user identities, providing a secure and scalable solution for accessing and processing image data.

We first provide an overview of image recognition technology and its applications, highlighting the importance of user authentication and access control in image recognition projects. We then introduce AWS Cognito and its key features, including user authentication and authorization, social identity providers, multi-factor authentication, and user management.

Next, we present a case study of an image recognition project that utilizes AWS Cognito. We describe the project's architecture, which includes an AWS Lambda function that processes images and videos based on user access and permissions managed by AWS Cognito. We provide a detailed analysis of the security and scalability of the AWS Cognito service and compare it to other user authentication and access control solutions.

Amazon S3

Amazon S3 (Simple Storage Service) is an object storage service provided by Amazon Web Services (AWS) that allows users to store and retrieve data from anywhere on the web. It provides developers with a simple web service interface to store and retrieve any amount of data, at any time, from anywhere on the web. The service is designed to deliver 99.999999999% durability and scale past trillions of objects worldwide.

Amazon S3 offers a range of features including scalability, security, durability, and accessibility. It provides a highly scalable, reliable, and cost-effective solution for storing and archiving data of any type and size. Users can choose from several storage classes, depending on their specific needs, including standard, infrequent access, archive, and intelligent tiering.

S3 stores objects, which consist of data and metadata, in buckets, which are logical containers for objects. Each bucket has a unique name that must be globally unique across all S3 accounts. S3 objects can be up to 5 TB in size, and there is no limit to the number of objects that can be stored in a bucket.

One of the key benefits of S3 is its security features. S3 provides several mechanisms to ensure that data is secure, including encryption at rest and in transit, access control through AWS Identity and Access Management (IAM), and bucket policies that control access to individual buckets. Additionally, S3 offers compliance programs that meet various regulatory requirements, such as HIPAA, PCI DSS, and FedRAMP.

S3 also provides a number of APIs and tools for managing objects and buckets, including the AWS Management Console, AWS CLI, and SDKs for popular programming languages such as Java, Python, and Ruby.

In summary, AWS S3 is a highly scalable, reliable, and cost-effective solution for storing and archiving data of any type and size. Its features include scalability, security, durability, and accessibility, and it offers several storage classes, security mechanisms, and APIs for managing objects and buckets.

Amazon Dynamodb

Amazon Web Services (AWS) DynamoDB is a fully managed NoSQL database service provided by Amazon that is designed to provide high performance, scalability, and flexibility to developers. It allows users to store and retrieve any amount of data, and it automatically scales to accommodate growing workloads.

DynamoDB is a document-oriented database, which means that it stores data in JSON-like documents. It is a key-value and document database that delivers single-digit millisecond performance at any scale.

One of the main benefits of DynamoDB is its ability to scale automatically to meet the demands of a particular application. This means that as an application grows, DynamoDB can automatically scale up or down to handle the increased or decreased workload. In addition, DynamoDB also provides features such as automatic partitioning, load balancing, and replication to ensure that data is always available and can be retrieved quickly.

DynamoDB also provides built-in security features, such as encryption at rest and in transit, and it integrates with AWS Identity and Access Management (IAM) for access control. It also allows developers to set fine-grained access control policies on individual items, which helps to ensure that only authorized users can access certain data.

Another key feature of DynamoDB is its ability to provide low-latency access to data. This is achieved through the use of SSD storage, which provides faster read and write performance compared to traditional hard disk drives.

DynamoDB also provides a flexible data model that allows developers to store and retrieve any type of data, including structured, semi-structured, and unstructured data. This makes it well-suited for a wide range of applications, including web and mobile applications, gaming, IoT, and more.

Overall, DynamoDB is a powerful and flexible NoSQL database service that is designed to meet the needs of modern applications. Its ability to provide high performance, scalability, and flexibility make it an ideal choice for developers who need to store and retrieve large amounts of data quickly and easily.

Application

The project addresses the growing need for improved security measures in the digital world, where sensitive information is stored and accessed remotely through online platforms. Traditional single-factor authentication (SFA) methods are no longer sufficient to prevent unauthorized access and potential breaches of data. MFA, on the other hand, provides an additional layer of protection to verify the user's identity before granting access to sensitive information.

The MFA system implemented in this project involves two layers of authentication: Google Authenticator and facial recognition using AWS. The Google Authenticator generates time-based one-time passwords (TOTP) that the user enters along with their login credentials. The TOTP expires after a set time, providing an additional layer of security. The second layer involves facial recognition technology that compares the current user to the authenticated user present in the record, which is verified by the organization at the time of sign-up.

The project's application can be significant in various industries that handle sensitive data, including healthcare, finance, and government agencies. By implementing a robust MFA system, organizations can significantly reduce the risks of cyber-attacks and protect their data from unauthorized access.

For example, in the healthcare industry, patient records contain sensitive information that must be secured from unauthorized access. A multi-factor authentication system using facial recognition technology can significantly improve the security of electronic medical records and reduce the risk of data breaches.

Similarly, financial institutions can use this system to secure their online banking services and prevent unauthorized access to customer data. The facial recognition technology provides an additional layer of security that ensures the user's identity before accessing their account.

Moreover, government agencies can use this system to secure their digital platforms, including online portals for taxes and other government services. The facial recognition technology can provide a higher level of security to protect sensitive information from unauthorized access and potential cyber-attacks.

Overall, the application of this project can be significant in enhancing the security of online resources and protecting sensitive data from cyber threats. It can be used across various industries and organizations to ensure that the right and authenticated person is accessing the data.

4. Literature Review

Digitalization is an important part of modern society. This digitalization includes the increasing use of online resources in daily life of people from communication to online payments or transition. This all data of accessing and communication to online resources are stored on remote locations such as cloud and data-bases, which has increased the demand of

security to ensure the right and authentic person is accessing the data. To solve these authentication issues for accessing the data, the security started from Single-Factor Authentication (SFA) has now gone to Multi-factor Authentication (MFA) or Two-Factor Authentication (2FA) [1]. Multi-factor authentication or two factor authentication is an extended security layer to your online resources after loggin in procedure. In this a customer after being logged in to any online environment is again authenticated using different methods. [2]
This multifactor authentication uses a strong combination of “Something you know”, “Something you have”, “Something you are” and “Somewhere you are” or “Someone you know”. This combination provide strong remote authentication mechanism which is harder for any unauthentic user to get access to any online resources. These multi factor authentication methods mainly uses more than one authentication methods, OTP or TOTP(Time-based One Time Password) and biometric methods such as facial recognition, fingerprint or retina scan. [3]

Research papers

1. The study conducted by Ometov et al. (2018) presents a comprehensive survey of multi-factor authentication (MFA) techniques. The authors highlight that MFA is increasingly being recognized as an essential tool for enhancing the security of online resources. The paper provides an overview of various MFA techniques such as password-based authentication, smart card-based authentication, biometric-based authentication, and knowledge-based authentication.

   The authors discuss the advantages and limitations of each technique and also identify the key challenges associated with MFA, including user acceptance, cost, and interoperability. The study emphasizes that MFA techniques need to be user-friendly, cost-effective, and interoperable to achieve widespread adoption.

   Ometov et al. (2018) also discuss the emerging trends in MFA, such as the use of wearable devices and context-based authentication. The authors argue that wearable devices such as smartwatches and fitness trackers can be used as authentication factors, and context-based authentication can provide an additional layer of security by considering various contextual factors such as location and time.

   Overall, the study by Ometov et al. (2018) provides a comprehensive survey of MFA techniques and highlights the importance of MFA in enhancing the security of online resources. The authors also identify the key challenges associated with MFA and discuss the emerging trends in this field. This study can serve as a useful reference for researchers and practitioners working in the field of cybersecurity and authentication.

2. In their paper "Two factor authentication", Mail and Box present a comprehensive overview of the concept of two-factor authentication (2FA), which has become increasingly popular in recent years as a means of enhancing security for various online services. The authors begin by discussing the shortcomings of traditional password-based authentication methods, which have proven to be vulnerable to various forms of attacks such as phishing, social engineering, and brute-force attacks. They then introduce the concept of 2FA, which involves the use of two distinct

authentication factors, typically something the user knows (e.g., a password) and something the user has (e.g., a token or mobile device).

The authors provide an overview of the various types of 2FA mechanisms, including one-time passwords (OTP), smart cards, biometric authentication, and mobile-based authentication. They also discuss the advantages and disadvantages of each approach, highlighting the importance of choosing the right combination of factors based on the specific requirements of the application or service.

One interesting aspect of the paper is the authors' discussion of potential attacks on 2FA systems, including phishing, man-in-the-middle attacks, and SMS-based attacks. They provide guidance on how to mitigate these risks, such as by using out-of-band communication channels or hardware tokens.

Overall, the paper provides a useful overview of the concept of 2FA and its various implementations, as well as the potential risks and mitigation strategies associated with these mechanisms.

The authors of the paper "Multi-factor authentication: A survey" did not use any specific tools in their research. Instead, they conducted a comprehensive survey of existing research on multi-factor authentication and analyzed the various methods and techniques used in these studies. They reviewed over 150 papers and organized the results based on the number of factors used in authentication, the types of factors used, and the authentication methods used. The authors used statistical analysis and visualization techniques to summarize their findings and provide a comprehensive overview of the state-of-the-art in multi-factor authentication.

3. The paper by Abhishek et al. (2013) provides a comprehensive study on multi-factor authentication schemes. The authors begin by highlighting the importance of multi-factor authentication in ensuring security in online transactions and access to resources. They note that traditional single-factor authentication mechanisms such as username and password are no longer sufficient in providing adequate security against advanced attacks.

   The authors go on to review various multi-factor authentication schemes, including those based on passwords, tokens, biometrics, and smart cards. They discuss the advantages and disadvantages of each scheme and provide examples of their implementation. They also examine some of the challenges associated with multi-factor authentication, such as usability, interoperability, and cost.

   The paper also highlights some of the emerging trends in multi-factor authentication, such as the use of mobile devices and social networking, as well as the integration of biometric authentication with other factors such as passwords and tokens.

   Overall, the study provides a valuable insight into the various multi-factor authentication schemes and their effectiveness in ensuring security in online transactions and access to resources. It also identifies areas for future research and development, particularly in improving the usability and interoperability of multi-factor authentication systems.

5. Research Gap

In recent years, there has been a significant increase in the number of cyber-attacks targeting web applications. These attacks can result in data breaches, financial loss, and damage to the reputation of businesses. To prevent such attacks, it is essential to implement multiple layers of security in web applications. The project addressed this issue by proposing a two-layer security approach that uses facial recognition and Google Authenticator.

Facial recognition technology is a powerful security tool that works by analyzing the facial features of an individual and comparing them against a database of known faces. The technology can quickly and accurately identify individuals, making it ideal for use in security systems. By incorporating facial recognition into the web application, the project aimed to add an extra layer of security that could prevent unauthorized access to sensitive information.

Google Authenticator is another security tool that provides an additional layer of security by generating a one-time code that is required for authentication. This code is generated on the user's mobile device and is required to complete the login process. This adds an additional layer of security by ensuring that only authorized users can access the web application.

The combination of facial recognition and Google Authenticator provides a strong two-layer security approach that can prevent cyber-attacks and unauthorized access to resources. The use of multiple layers of security is becoming increasingly important as cyber-attacks become more sophisticated and frequent.

One potential application of this project could be in the financial sector, where the security of online banking and financial transactions is critical. The two-layer security approach proposed in the project could be used to secure online banking applications and prevent unauthorized access to sensitive financial information.

Another potential application could be in the healthcare sector, where the security of patient data is of utmost importance. By using the two-layer security approach, healthcare providers can ensure that only authorized personnel can access sensitive patient information, preventing data breaches and protecting patient privacy.

Overall, the project's approach to adding an additional layer of security to a web application using facial recognition and Google Authenticator provides better protection against cyber-attacks. The use of multiple layers of security is becoming increasingly important, and the project's approach can be applied to various industries to secure web applications and prevent unauthorized access to sensitive information.

6. Problem Statement

In a rapidly growing technology environment, threats related to technology and its security are also increasing accordingly. Hence to make accessing to any web-application more secure, web application provider can use multi-factor authentication mechanism that uses face recognition to ensure that the data is consumed by legitimate user,

7. Motivation

Multifactor authentication (MFA) has become increasingly important in today's digital world, where online security threats are a growing concern. MFA adds an extra layer of security to the authentication process by requiring users to provide multiple forms of authentication, such as a password and a security token or biometric data.

Facial recognition technology has also seen a significant increase in popularity and adoption, particularly in the fields of security and surveillance. With the rapid advancements in computer vision and deep learning algorithms, facial recognition has become a reliable and accurate method for identifying individuals.

the motivation for this project is to investigate the feasibility, security, and usability of facial recognition-based MFA as a potential solution for enhancing online security and improving user experience.

8. Objectives

- AWS COGNITO si used to deploy the web page and its login page to ensure the identity and authentication of the srevice.
- AWS Rekognition to make a collection of images to identify the legitimate user along with their corresponding labels. Which is triggered whenever an image is stored in S3, lambda function is used to triggered to generate faceprint using AWS Recognition.
- To secure that web app using AWS cognito and facial recognition using the AWS Rekognition collection.
- To secure teh data and to store the user input in S3 bucket along with their mata-data, that will help in storing the images in DynamoDB along with their faceprints.

8. Methodology

- We use the service called Cognito to deploy a web app on AWS and secure it using the MFA using the same.
- Cognito will send the Time based one time password on to the email the user is registered with.
- Once they are logged in the user will use google authenticator to register themselves.
- If they want to log in to the web app again they would have to use the key provided to them by the google authenticator.
- when the user first login, they need to provide a picture of themselves, which is stored in S3 alon gwith their mata-data.
- Everytime any picture is stored in S3 it triggers a Lambda Funtion that generates a faceprint using AWS Rekognition
- These faceprints are stored in DynamoDB along with the images.
- Now, whenever a user logins an image is stored in S3 with is then compared with the face prints present in the DynamoDB.

9. PERT Chart

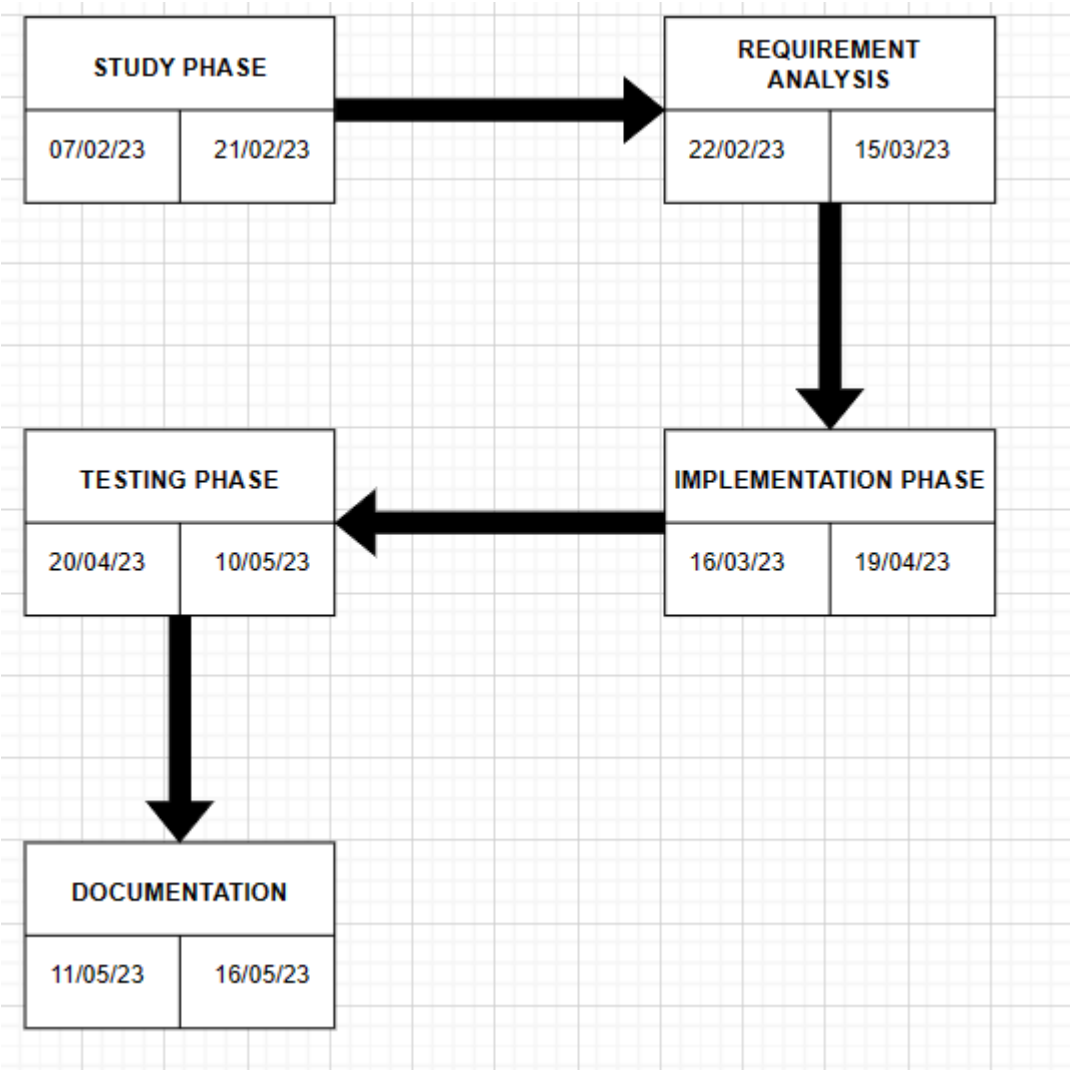

Fig 1: PERT Chart

10. References

1. Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. and Koucheryavy, Y., 2018. Multi-factor authentication: A survey. *Cryptography*, *2*(1), p.1.
2. Mail, A.O.L. and Box, D., 2017. Two factor authentication.
3. Abhishek, K., Roshan, S., Kumar, P. and Ranjan, R., 2013. A comprehensive study on multi factor authentication schemes. In *Advances*

in Computing and Information Technology: Proceedings of the Second International Conference on Advances in Computing and Information Technology (ACITY) July 13-15, 2012, Chennai, India-Volume 2 (pp. 561-568). Springer Berlin Heidelberg.

11. Conclusion and Features

Facial recognition technology has gained significant attention in recent years as a powerful tool for enhancing security in various settings. This project aims to contribute to the efforts of improving security by providing an additional layer of authentication using facial recognition. By comparing the current user's facial features to the authenticated user's facial features present in its record, the system ensures that only authorized users can access the resources.

One of the key features of this project is its ease of use. Facial recognition technology eliminates the need for users to remember and enter complex passwords, making it more convenient and efficient. Moreover, the system provides an added layer of security to resources, reducing the risk of unauthorized access and data breaches.

Another feature of this project is its scalability. The system can be integrated into various organizational settings and can handle large volumes of users. This makes it suitable for deployment in organizations of different sizes, from small businesses to large corporations.

In addition, the facial recognition system used in this project is highly accurate and reliable. It uses advanced algorithms to analyse facial features, ensuring that the system can distinguish between authorized and unauthorized users with a high degree of accuracy. The system can also adapt to changes in facial features over time, such as aging or changes in hairstyles.

In conclusion, this project provides an additional layer of security using facial recognition technology. The system is easy to use, scalable, and highly accurate, making it a valuable tool for organizations and individuals seeking to improve their security. By implementing this system, users can enjoy enhanced security and convenience, while organizations can reduce the risk of data breaches and unauthorized access to resources.

12. Implementation

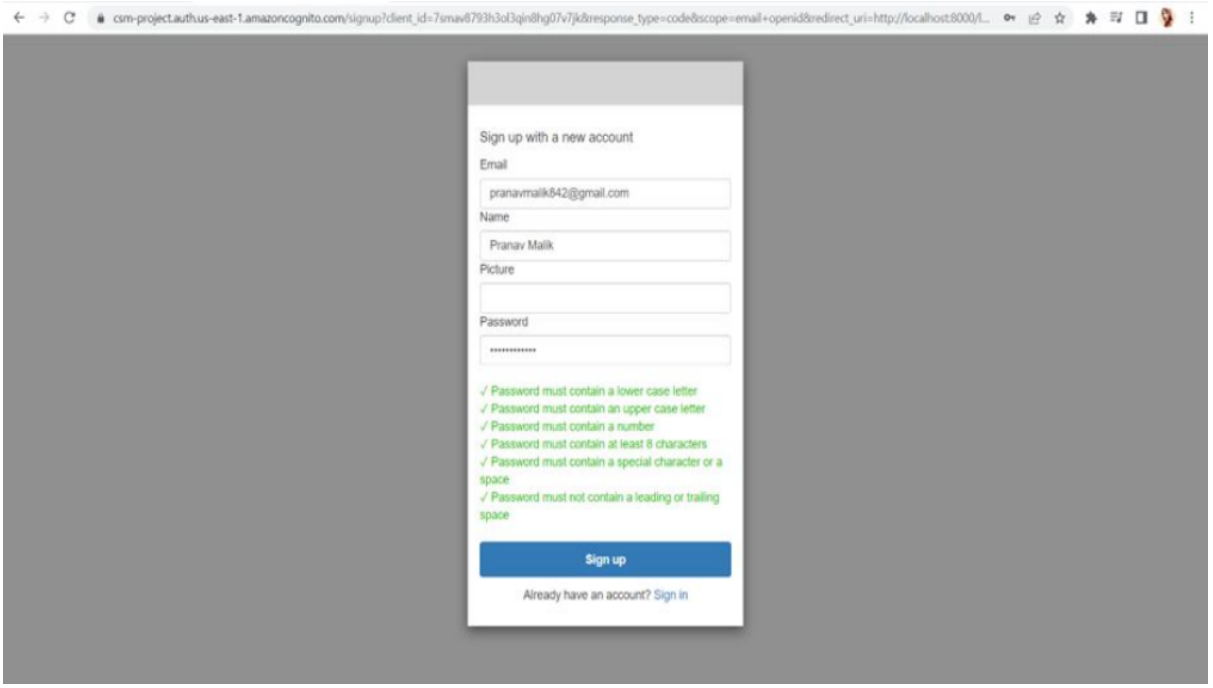

Fig 2: Signup page

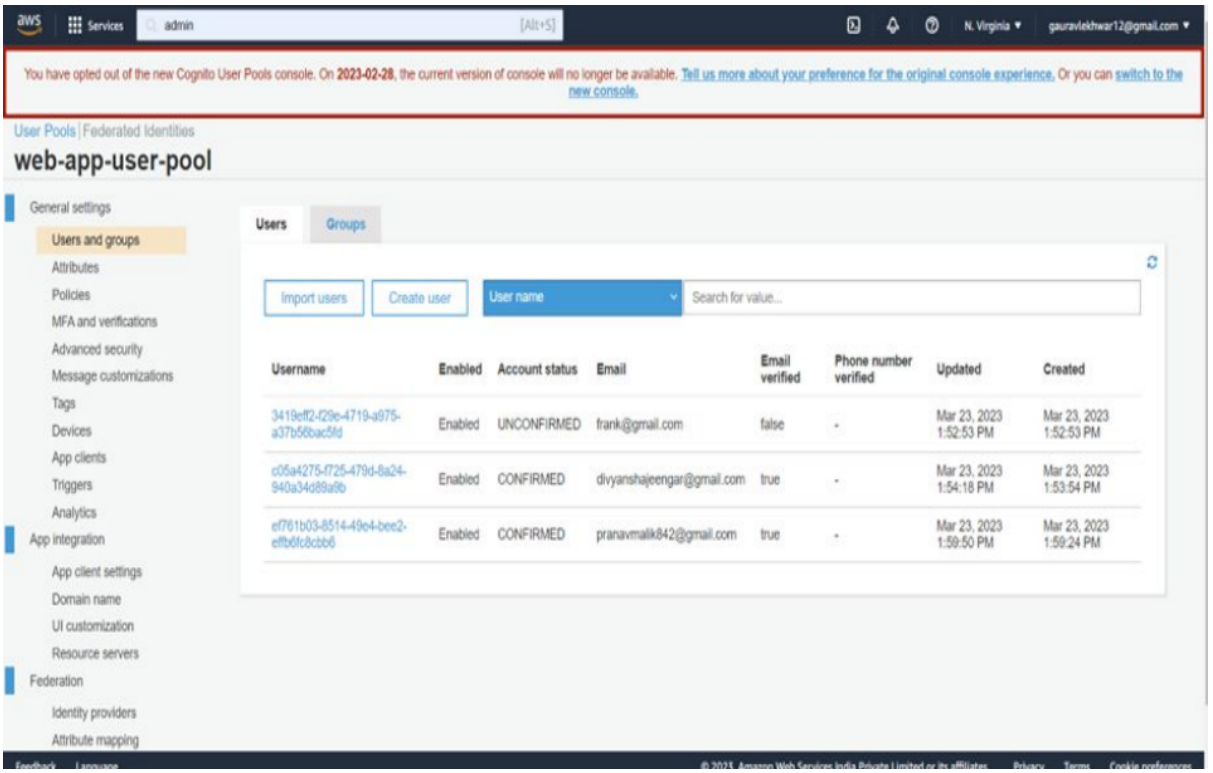

Fig 3: list of signed in people

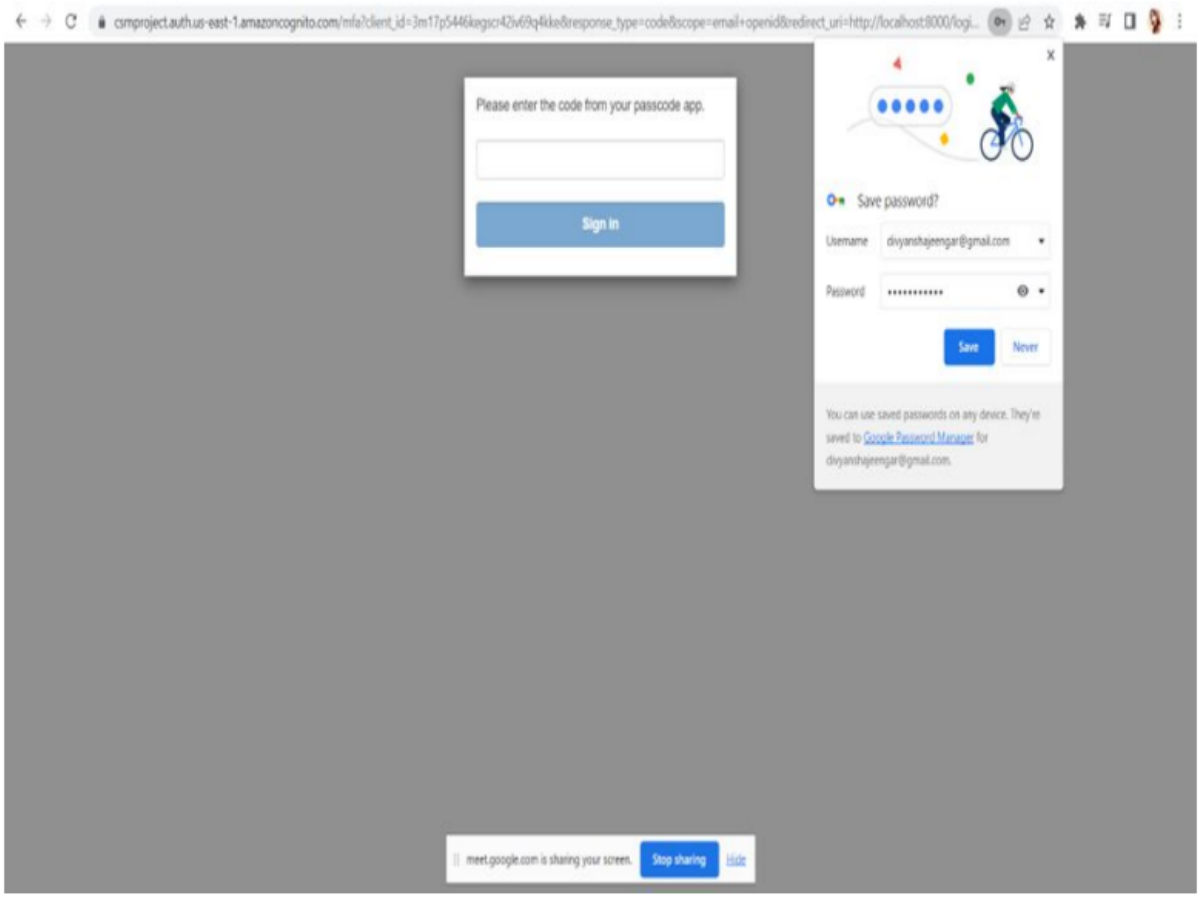

Fig 4: multi-factor authentication

Fig. 5. Logged in

Fig.6. New login page

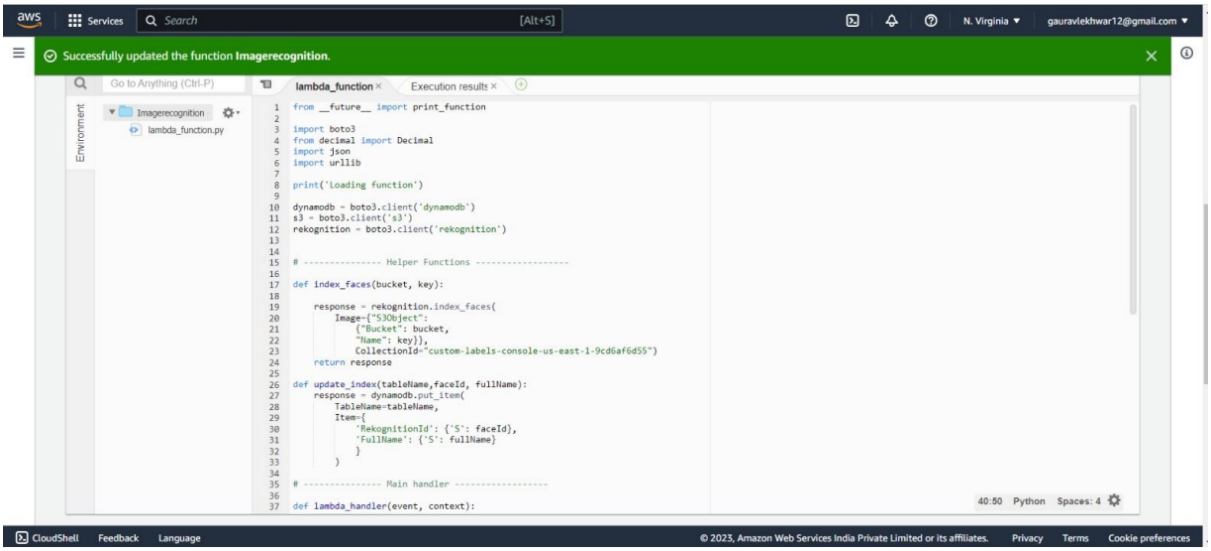

Fig 7. Lambda function

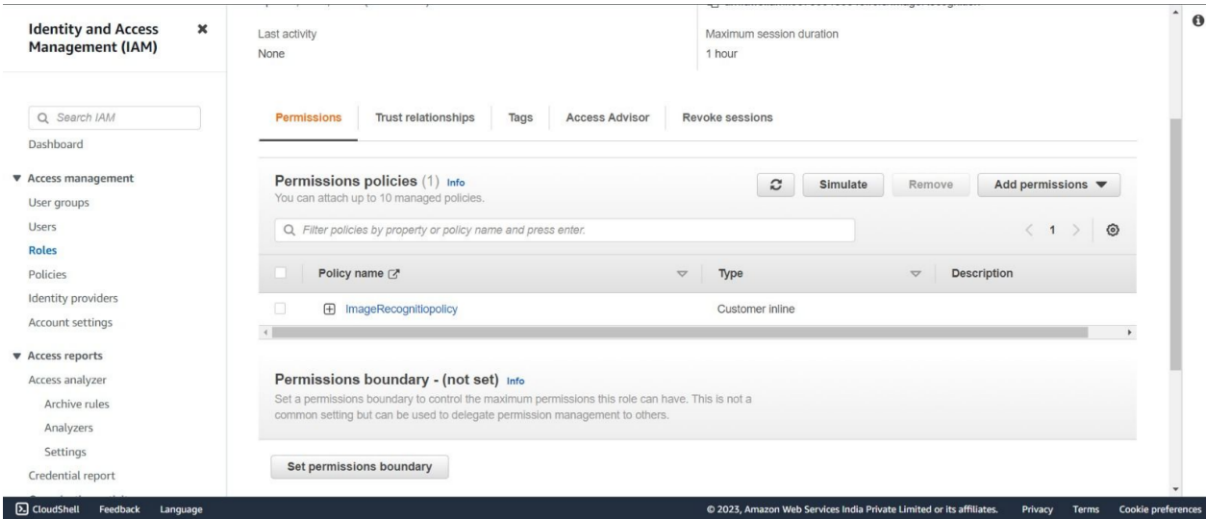

Fig.8. IAM role