Enhancing Cloud Security through Integration of Three-Factor Authentication and Role-Based Access Control

MSc Research Project
MSCCYB1

Srushti Jadhav
Student ID: x21211973

School of Computing
National College of Ireland

Supervisor: Joel Aleburu

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Srushti Jadhav		
Student ID:	X2121973		
Programme:	MSCCYB1	**Year:**	September 2022-23
Module:	MSc Research Project		
Supervisor:	Joel Aleburu		
Submission Due Date:	14/08/2023		
Project Title:	Enhancing Cloud Security through Integration of Three-Factor Authentication and Role-Based Access Control.		
Word Count:	4439 **Page Count** 19		

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Srushti Jadhav

Date: 14/08/2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Enhancing Cloud Security through Integration of Three-Factor Authentication and Role-Based Access Control

Srushti Jadhav
x21211973

Abstract

In the evolving generation of digital identities, ensuring secure access to cloud computing resources is predominate. Cloud computing offers large benefits but also come with security challenges. Authentication and authorization are two important pillars of identity and access management. This research work discusses integrated approach towards combining multilayered security concept to existing multifactor authentication system and user specific roles access granularity mechanism by studying security principle of least privilege and separation of duties on organizations and business those who are leveraging Amazon web service. The design implementation of research work carried out on cloud resource level which evaluates effectiveness in enhancing clous security.

1 Introduction

Background:

In today's digital booming world, Organizations and businesses are shifting their set up in cloud computing environment. This move is rapid and depends on variety of entities. Cloud services offers more scalable, flexible, cost effective environment to grow their operation and business fast in globally dynamic market. Investing in cloud resources than setting up own on-premises servers is always profitable and productive. As many organizations use large quantity of computational resources, they can leverage it on cloud and adapt pay as you model. Cloud computing comes with challenges. Organization stores their important and private data on cloud, securing this data is essential. Due to remote services offered by cloud also makes these organizational data susceptible to the cyberattacks like unauthorized access and execute malicious tasks within system can be harmful which breaks trust chain between client and service provider. (Lysakov, Sievierinov and Taran, 2021)

Identity and access management verifies that only authenticated and authorized people have access to the specific information in cloud. This is managed by using password policies and MFA, assigned user specific roles and user account management. First part which is Identity management handles user's identity while access management deals with provisioning and deprovisioning user's access to resources. (Pinki et al., 2014)

Due to digital transformation in industry leads to adoption of cloud computing resources to store, process and manage their data ensuing security. The conventional password based authentication system seems to be outdated because of vulnerabilities associated with it.

Advanced authentication mechanisms such as multifactor authentication and three factor authentication can be helpful to strengthen the security measures for accessing cloud services. 3FA is the additional layer on top layer of MFA which can achieved by using biometric attributes of user like face recognition or fingerprint or iris recognition.

To reduce security risks related to unauthorized access, least privilege principle can be used which means giving user access only to resources required to perform his role. Similarly, Separation of duties is also a security principle which ensures any person have does not have elevated access also job roles of each individual should be separated and access given accordingly based on their work. Role based access control model offers structured approach to manage these principles ensure right entity have right access. (Wei Li et al., 2012)

Problem statement:

Research Question: Why it is needful to implement advanced security mechanisms such as MFA and RBAC together, especially for roles with elevated privilege?

As organizations migrating their operations to cloud, it is challenging to import security and access control to the computing resources. When there is concern about privileged users such as admins and managers, cyber attackers mainly target these users to gain private data and escalates privileged access. Simple authentication techniques seem weak and insufficient towards advanced types of breaches. If there is no structured access control, authenticated users also go beyond their scope intend to perform malicious activities. To address this issue and building trust between service provider and client to ensure compliance is important also for data protection. This can be achieved by integrating enhanced security tactics like strong authentication approach like assigning MFA and 3FA to the role specific entities so that role based access framework also can be implemented. This is one of the powerful approaches for implementing security on resource/data level if using cloud services.

Objective:

The main goal of the research to examine and explain multilayered security in any organization who utilize cloud products in their web environment. Some of objectives discussed below:

- Understand and analyse security needs, risks and vulnerabilities associated if using cloud services, especially for the user roles with extra rights to perform activities.
- Exploring and Investigating design flow of enhanced authentication structure such as MFA and 3FA withing cloud environment.
- Examine post authentication process and role specific access control system for appropriately handling access to resources according to designated role. Review security benefits of combining strong authentication and authorization system.
- Evaluate friendly user experience along with security measures so that accessibility and ease of use cannot be compromised.

2 Related Work

The SensiPass® developed new feature where Microsoft Azure Active directory can be collaborated which is markable advancement in field of identity and access management. This paper describes that SensiPass® has designed new API which can be integrated with Azure. Azure's conditional access policy has also been used for analysing user's access to application. Together they provide IDaaS solution (identity as a service) which provider layered and robust security to their clients. The paper merely discusses about SensiPass® architecture, its integrating API features with Azure active directory, Authentication design flow, managing digital identities and this whole system defends various types of attacks. (Kaushik, 2021)

This paper discusses about CAPTCHA system which has been acts as foremost defense for Bots. The traditional CAPTCHA system has limitations for cloud environments. Further it discusses types of attacks related to password such phishing, keyloggers, dictionary attacks, etc. To mitigate, enhanced CAPTCHA system has been developed which involves replacement of conventional CAPTCHA with replacement of characters which allows user to use new password for every session. This replacement of characters depends on client -server agreement. Salted hash mechanism on password has been used for signing in methods. This has been proposed in Windows 10 operating system using Node.js, Mongo DB and HTML. This paper provides valuable insights for building authentication and address vulnerabilities related to password attacks. (Althamary and EL-Alfy, 2017)

Facial recognition is integral part of multifactor authentication process which provides identity verification of individual entity. This paper develops automatic facial recognition system. Deep Neural network and amazon rekognition is used to analyze the image for accuracy and efficiency. The attendance system has been developed highlighting biometric technology to differentiate between humans and bots. The faceprint can be matched with images which is stored in S3 with use of metadata and AWS rekognition. This paper endeavors advancement in Biometric authentication factor using AWS cloud services adds extra layer of security. (Gupta et al., 2022)

The work proposes the 3-level multifactor authentication scheme which includes out of band authentication as one factor that robust defence against man in middle attack. The first level process includes use of username and password with double encryption using SHA-1 and AES128-CBC, second level includes OTP verification, and third level has graphical screen interaction with no. of clicks on images, buttons and menu items. This paper introduces graphical authentication system which rely on clicking the specific point on screen by user to get access to resource. User gets hint for this sequence on their mobile phone or device. 3 level password authentication scheme uses images, colour pixels and OTP which are encrypted. As discussed in paper, this factor gives new shape to authentication and digital identity. (SINGH and SINGH, 2019)

Five factor authentication mechanism extends to three factors has been developed within corporate network based on Microsoft azure active directory network with only small implementation cost. Five factors of authentications are as follows- Username and password, smart card or token, biometric such as fingerprint or faceprint, geolocational information and time factor. CredSSP is used as credential security service provider and Winlogon provides infrastructure. This paper describes strengthening user authentication process in network service which improves security model. (Kadlec, Jaros and Kuchta, 2010)

The paper introduces the concept of role base access control model to maintain principle of least privilege tailored for industrial machines to have remote maintenance. The concept is developed on Linux system using framework. By using security modules in Linux like AppArmor which enables MAC on linux system. Later, it describes it is possible to implement MAC with RBAC. In this user is linked to individual instance. Based on roles required to perform maintenance specific task, role profiles are added in servicebash. Overall, this paper suggests by limiting user access, security impacts can be minimized. (Kern and Anderl, 2018)

The paper literature discussed about design and implementation of Access control as a service mainly focus on RBAC in AWS. This allows cloud customers to use and integrate service seamlessly by enforcing RBAC policy inside amazon web services. The paper provides foundational understanding of access control issues inside cloud. This gives in depth structure of access control as a service and discuss about its key elements like policy administration point, policy decision point and policy enforcement point and integration between these components. This architecture is easily adaptable to various cloud infrastructures especially those who use web services. The paper describes current access control architecture in AWS and its IAM policies for RBAC. (Wei Li et al., 2012)

3 Research Methodology

Motivation:

Authentication and Authorization are two fundamental factors of identity and access management. Authentication verifies the identity of user to access the system or resources. According to guidelines provided by The National Institute of Standards and Technology (NIST) there are main ways to check a user's identity: something you know (logon id and password credentials), something you are (Biometric), something you have (email/OTP tokens) are factors of authentication Authorization ensures the access of authenticated user. Once user proves identity, authorization is process of checking if user is allowed to perform specific task or not. Permissions, roles and policies are main components of authorization. Authentication is part of identity management whereas Authorization belongs to access management. With robust authentication and correct authorization, only right individuals are accessible to the sensitive data/resources within organization. Strict regulations within organization implied compliance, security. It simplifies audit process by tracking who and when accessed resource. (Kaushik, 2021)

Cyberthreats discussed if authentication and authorization mechanism is weak:

• **Credential theft/Unauthorized access:** If attacker gains user's credentials like password cracking/stealing or any factor of authentication even if RBAC is implemented, they can access resource assigned to user's role. Shoulder surfing techniques can be used to steal credentials.

• **Phishing attack:** Users are tricked to provide their credential by using malicious entities. Social engineering techniques used here.

• **Session Hijacking:** Session tokens are intercepted, and attackers impersonates as the user.

• **Insider threat like privilege escalation:** These refers to malicious or unintentional actions taken by employees, contractors, business associates or any other person within organization if roles are improperly defined.

• **Misuse of permission**: If users are assigned with broad range of roles, they or anyone with their credentials misuse permission.

• **Data Exfiltration:** Once unauthorized user gets inside the system, they can extract sensitive which leads to the confidentiality breach.

•**Replay attack:** If attacker captured authentication tokens, they can interception authentication process.

•**Brute force attack:** It is process of guessing and attempting all possible ways of combination of characters until correct password is found.

• **IAM policy exploits:** If policies assigned to IAM role are more and if attackers gain access to system, attacker can perform malicious activity.

To prevent unauthorized access and potential attacks in cloud environment, security measures should be considered discussed below-

Security enhancement with layered authentication:

Traditional authentication (User id and password) mechanism can be replaced with two factor and three factor authentication and Three factor authentication. In three factor authentication, third factor depends on user's biometric entities which cannot be used by anyone else. By using three factor authentication for elevated privileges, significantly risk of unauthorized access is reduced. Even if one or two factors of authentication are bypassed, third authentication factor serves as additional wall. Physical attributes of user are unique which are reliable and quick for biometric authentication.

Least privilege principle:

The principle ensures the user of organizations have minimum level of access to resources to perform only specific tasks assigned to user. This can be achieved by regularly review and update IAM policy to make sure end user review access. Role based IAM permission is way to accomplish least principle of least privilege. (Kern and Anderl, 2018)

Session Duration:

Set shorter session duration especially for elevated role to minimize attack vector.

Tokenization:

Generating tokens to grant temporary access to cloud resources assuming IAM roles which represents user's permission without exposing real credentials and other sensitive information. Token issued for some time and after certain time using, it gets expire. This mechanism ensure security.

Multilayered security model along with strong and customized authentication mechanism based on role of user is robust approach. Security procedure which includes 3FA and RBAC together ensure authorized users have access to right entity. Such security system can be designed to provide rigid security.

Use case:

Primary entity: End users

Stakeholders and other participants:

- Cloud service provider – It can be used as identity provider for authentication and role specific access to resources according to organizational needs. For example, AWS, Google cloud, Microsoft Azure.
- End user – Users who wants to access cloud resources/services from their web application.
- Admin- Person who assigns/revokes the permissions to end users according to their role so that user goes through the authentication process which has been implemented according to role.

Case scenario:

Preliminary conditions:

There are two types of end users specified according to their job role. User 1 have been assigned with Role 1 and User 2 have been assigned with Role. Both the users are consuming cloud resources for performing their job. No user has full access or root access to any of cloud service to ensure compliance. Consider User 1 is normal user and User 2 does managerial tasks to do so user 2 is having extra privileges or access to more additional cloud resources.

Main flow:

Both the users undergo through the authentication provided by identity provider to access cloud services. Roles which should assigned to two different users are defined using IAM role. User 1 follows two factor authentication and User 2 follows three factor authentication as user 2 have access to extra resources to avoid privacy breach or cyberthreats like password-based attacks, credential hacks. Even if user 1 gets the credentials of user 2 by using brute force or any other insider cyberattack techniques, User 1 must follow through three factor authentication where third factor will be biometric authentication which is totally based on physical attributed of User 2.

Post conditions:

Role based access control can be implemented to avoid privilege escalation. With this user case, principle of least privilege, separation of duties and with stronger authentication mechanism, multilayered security approach is followed.

Amazon web service:

In cloud computing market, AWS has been always a leader because they offer seamless interoperability and better integration within their different services. AWS has large global network of data center with high availability among services. AWS provide broad documentation, support services and tutorials for implementing and troubleshooting difficult use cases. AWS provides wide range of security tools. They also have detailed cost management and budgeting tools which allows anyone to manage expenses according to pay-as-you-go model. (Sailakshmi, 2021)

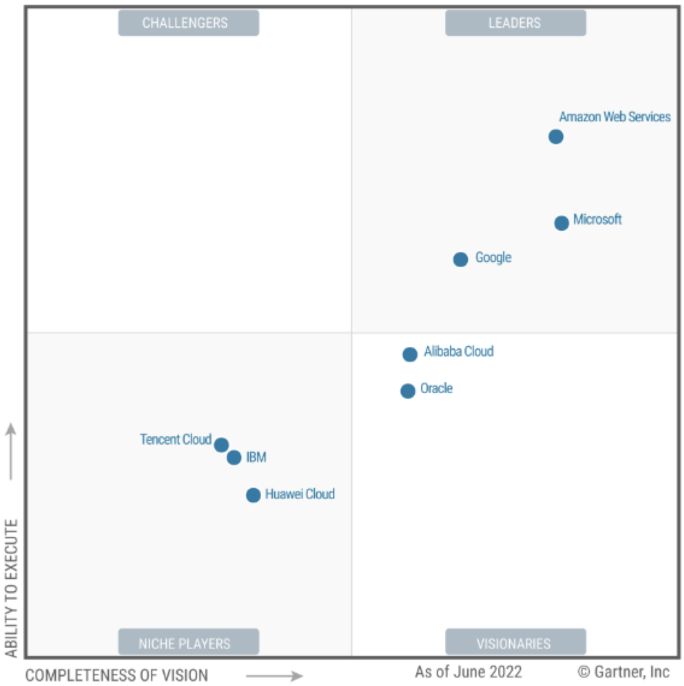


Figure 1. Magic Quadrant for Cloud Infrastructure and Platform Services (aws.amazon.com, 2022)

By considering above use case, AWS is more preferrable for implementation over other cloud platform their services are easily integrated with the use of different API. All the services mentioned below and some other addition to it can be used to build a stronger authentication along with role-based access control. (Amazon, 2019)

AWS IAM: One of the strong web services provided by AWS which helps in managing user and their permissions to access resources. By using AWS IAM, AWS users and group can be created and with assignment of proper permission, we can allow or deny access to user. Along with that we can assign permission to AWS resources as well by creating IAM role so that we can restrict permissions. Poilcies specifies permissions to access resources which can be attached to users, groups and IAM roles. It enables the MFA and provide define password requirements. There are pre-defined Service linked IAM roles are also available which allows interaction between AWS service any other resource on AWS.

AWS Cognito: It works similar like other identity providers in market such as OKTA, PingID, etc. It creates user pool for user management and also identity pools can be created with temporary access credential of AWS to other identity providers. Cognito is very flexible and have great integration capabilities to integrate with other AWS services and other web applications. AWS Cognito have facility to build custom authentication as per business requirement and flow.

AWS Rekognition: Rekognition can used to do analysis of image and videos. It has advanced capabilities to do facial recognition and can directly integrated with other AWS services. This is very helpful AWS service to build biometric authentication.

AWS SDK: It provides bigger range of programming languages and interface which makes any application and AWS resource to integrated with AWS SDK easy.

4 Implementation

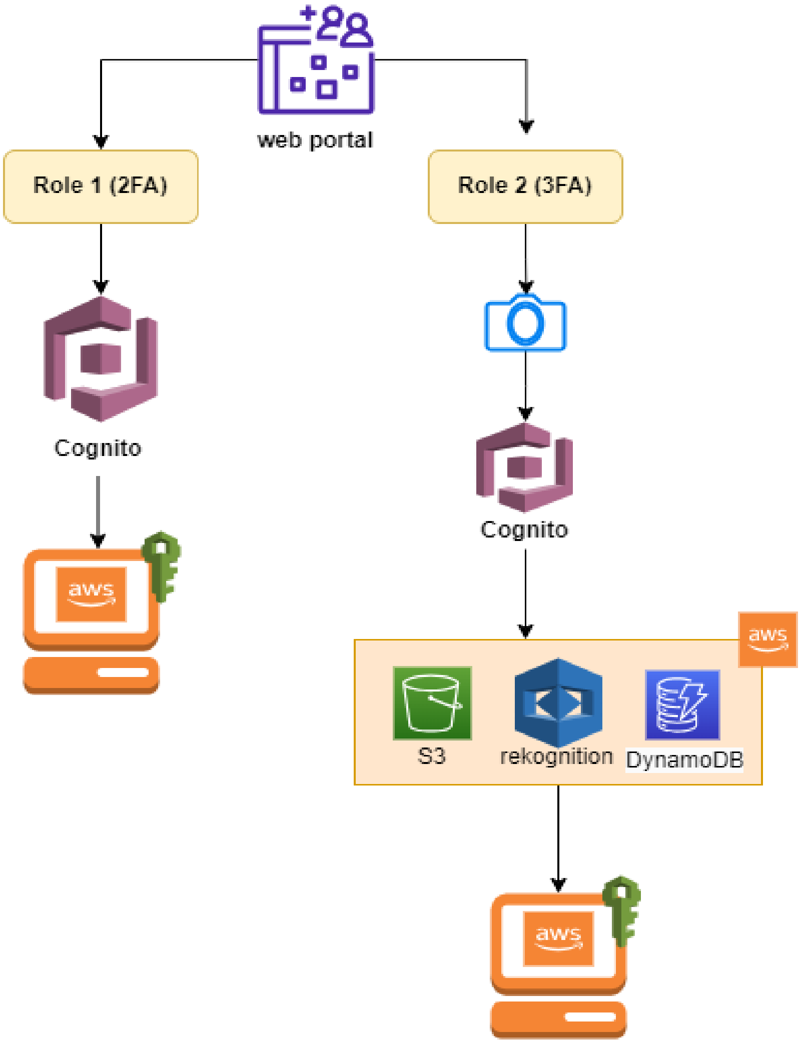


Figure 2. Architecture

One web page is developed by supposing through which users are accessing cloud resources. For this implementation, we just have assumed two role of users- Role 1 and Role 2. According to use case, suppose role 1 user has access to some resources and Role 2 users have access to extra cloud resources than role 1 users.

Both roles need to go through authentication to verify their identity. So here for authentication purpose, AWS Cognito has been used. AWS Cognito is used as identity provider. Both the users access the web page, suppose from their organizational portal (who is using cloud products for their business) which is redirecting them to use cloud service. There on portal, User must select their role defined by their organization to perform computational task. Computational resources required for their task has been defined in AWS IAM role to define concept of RBAC. IAM roles has been created with specific services along with permission added. Two separate roles have been created for Role 1 and Role 2.

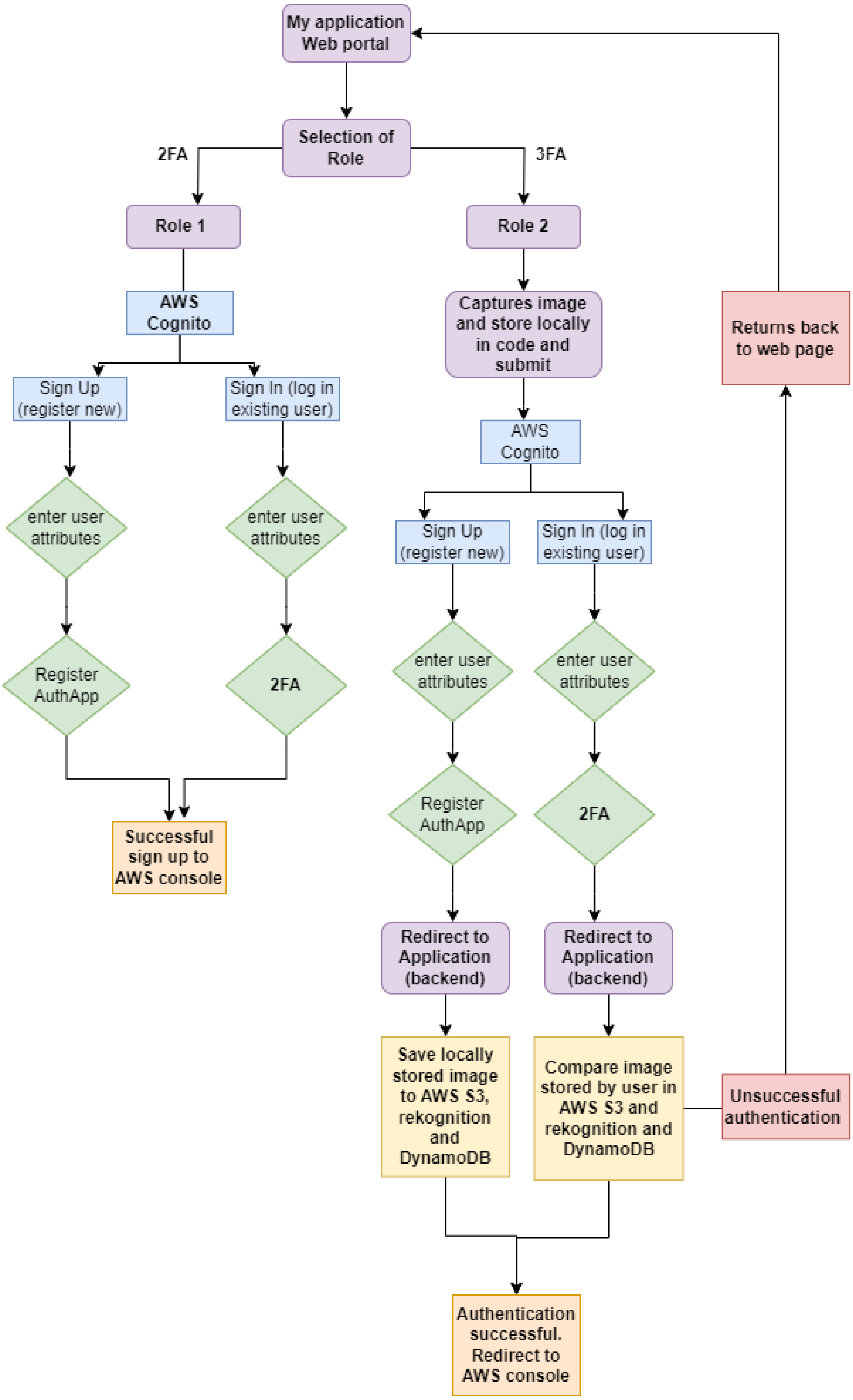
If user is selecting role 1, AWS Cognito is providing them authentication window as there is feature in AWS Cognito of app integration. For this purpose, user pool is created in AWS

Cognito. If user is new, then same service will give sign up feature. For sign up process, there is facility to add as many attributes regarding user information such as username, email id, birthdate, Gender, mobile number, etc. If user is already registered, user follow login process. In user pool created, we enable MFA for users so that user goes through multifactor authentication which follow two factor authentication process. First factor of authentication is userid (email id) and password and second factor of authentication is token/OTP which has been linked with user's authenticator app. Once user of role 1 passes through all these factors, user will get temporary token from AWS assuming IAM role so that user can utilize cloud resource. Hence role 1 users follow two factor authentication process.

If user is selecting role 2, again AWS Cognito is providing authentication window but here flow of authentication has been customized. As discussed in use case, role 2 have elevated privilege as role 2 user perform managerial task. Here extra layer of authentication has been added to restrict unauthorized access. Authentication flow is decided in backend code. During sign up process image of user is captured through web cam and stored locally for further processing. When user submits role 2, AWS congito provides identity window for sign up or sign in process. When user selects sign up, AWS cognito provides all the attributes that are required for new account creation along with two factor authentication entities. After this process user is directed to code in backend where the locally stored image of user is uploaded to AWS S3 bucket and AWS DynamoDB for metadata. After successful upload of image, User is redirected to AWS console with roles assigned by IAM to user. For sign in, two factor authentication process is same provided by cognito. Now, for biometric authentication image of user is again uploaded to S3 bucket. There is existing image of user uploaded during sign up which is used as target. With the help of AWS rekognition, both these images are compared and rekognition verifies and returns similarity index of those images to application. Based on percentage of similarity index, application allows user to sign in or deny. Due to flexibility, AWS SDK for programming interface which provide vast library of API's is used rather than lambda function to avoid complexity of flow.

These temporary access tokens are generated by AWS assuming IAM role with the use of API AssumeRole. Here the implementation has been done using python programming language in backend and integrated it with AWS API to follow required flow and to achieve objectives of research. Here there is no dependency for authentication on third party identity providers such as okta, pingID, ForgeRock so that there is no need to pay for subscription. AWS services are used to develop our required authentication mechanism and as AWS is flexible it can be integrated with any application. This research has been carried out practically to achieve multilayered security along with role based access control which is always enhanced approach. With this method, separation of duties and least privilege principle also has been followed.

5 Design flow



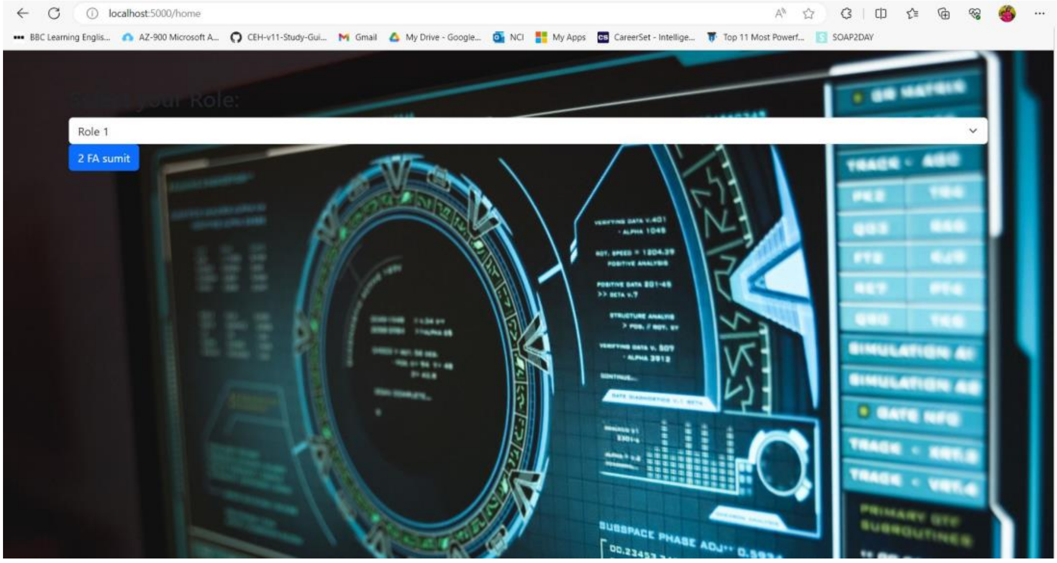
My application Web portal
Selection of Role
2FA
3FA
Role 1
Role 2
AWS Cognito
Sign Up (register new)
Sign In (log in existing user)
enter user attributes
enter user attributes
Register AuthApp
2FA
Successful sign up to AWS console
Captures image and store locally in code and submit
AWS Cognito
Sign Up (register new)
Sign In (log in existing user)
enter user attributes
enter user attributes
Register AuthApp
2FA
Redirect to Application (backend)
Redirect to Application (backend)
Save locally stored image to AWS S3, rekognition and DynamoDB
Compare image stored by user in AWS S3 and rekognition and DynamoDB
Authentication successful. Redirect to AWS console
Returns back to web page
Unsuccessful authentication

Figure 3. Flow diagram

6 Evaluation

This area of paper describes test cases of implemented architecture. It involves several experimental discussions of results after successful authentication of two factor authentication, three factor authentication, unsuccessful authentication and redirection of successful authentication to AWS console specific to IAM role assigned to users of Role 1 and Role 2.

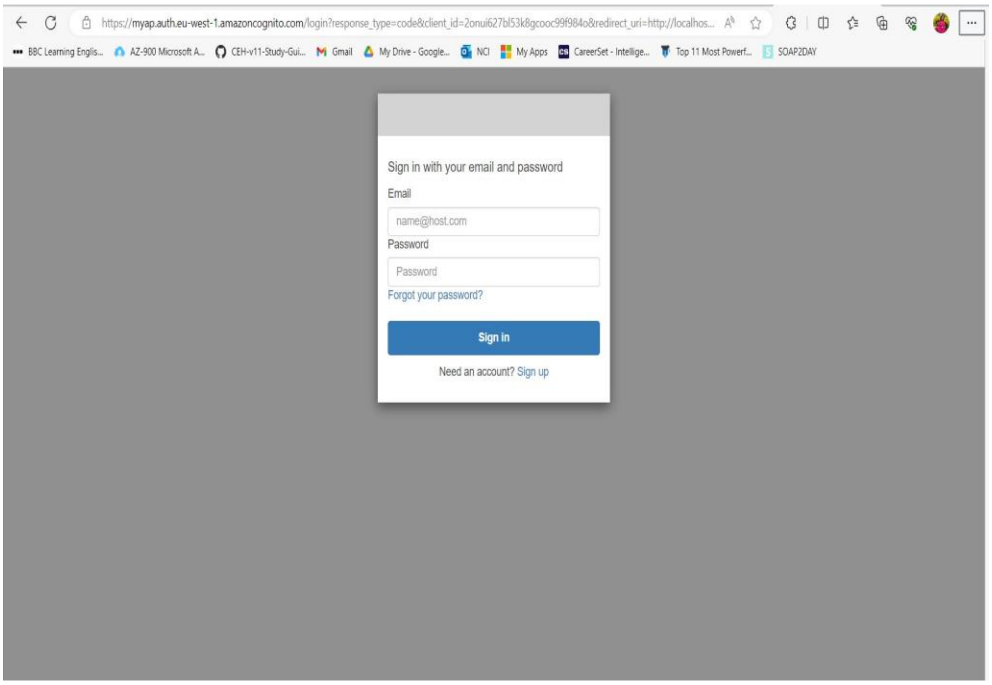
6.1 **Test case 1 -** If user of role 1 successfully undergoes two factor authentication provided by AWS Cognito.


localhost:5000/home

Select your Role:

Role 1

Figure 4. login page


https://myap.auth.eu-west-1.amazoncognito.com/login?response_type=code&client_id=2onui627bl53k8gcooc99f984o&redirect_uri=http://localhos...

Sign in with your email and password

Email

name@host.com

Password

Password

Figure 5. Cognito window

6.2 **Test case 2-** If user of role 2 successfully undergoes three factor authentication provided by AWS Cognito and web interface**.**

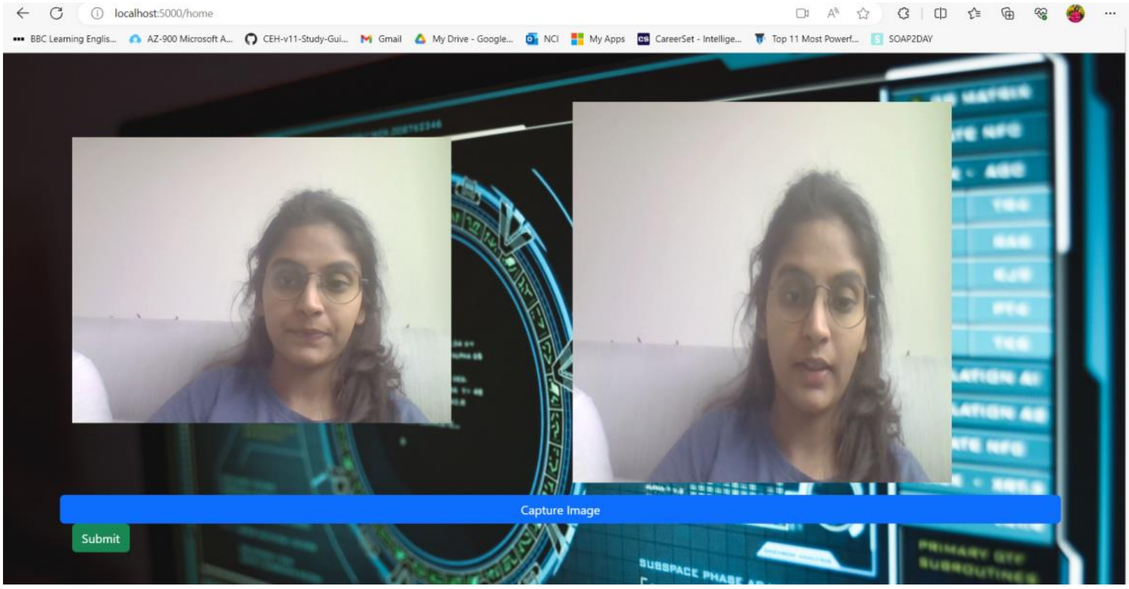
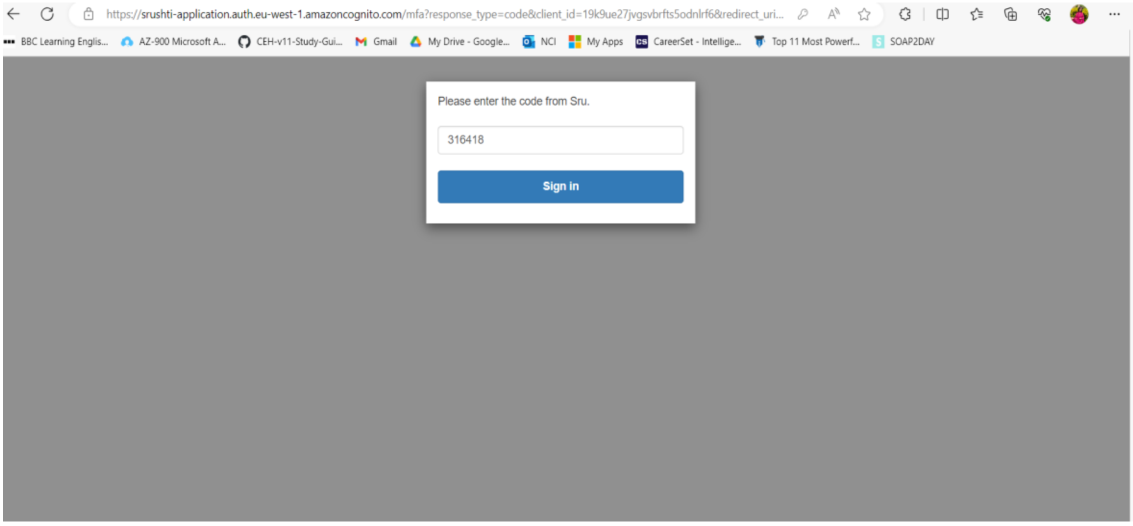


Figure 6. Biometric verification



Please enter the code from Sru.

316418

Figure 7. 2FA

6.3 **Test case 3 -** If user of role 2 does not validate through three factor authentication and unsuccessful to get access to AWS console assigned to their role. Users are redirected to homepage.

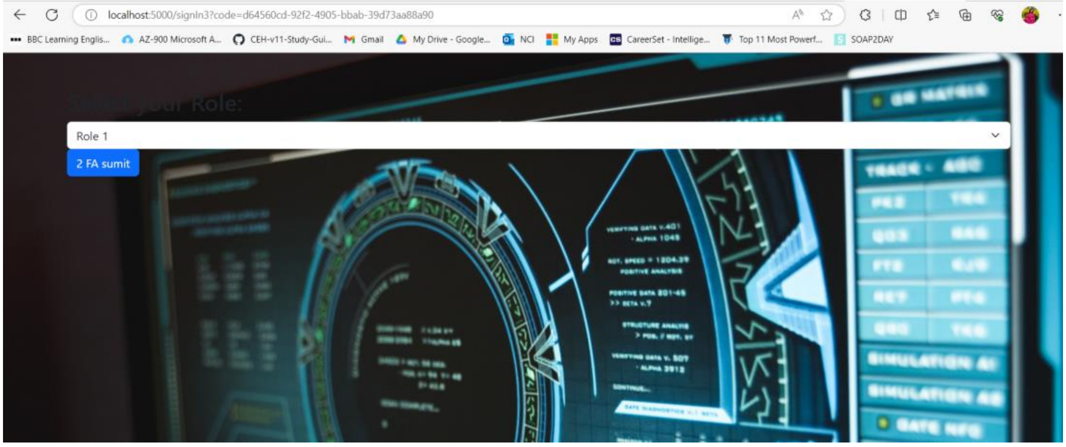

localhost:5000/signIn3?code=d64560cd-92f2-4905-bbab-39d73aa88a90
Select your Role:
Role 1
2 FA sumit

Figure 8. authentication failure

6.4 **Test case 4 -** If users of both roles successfully get through authentication process, they will be redirected to AWS console with specific role assigned to users using AWS IAM.

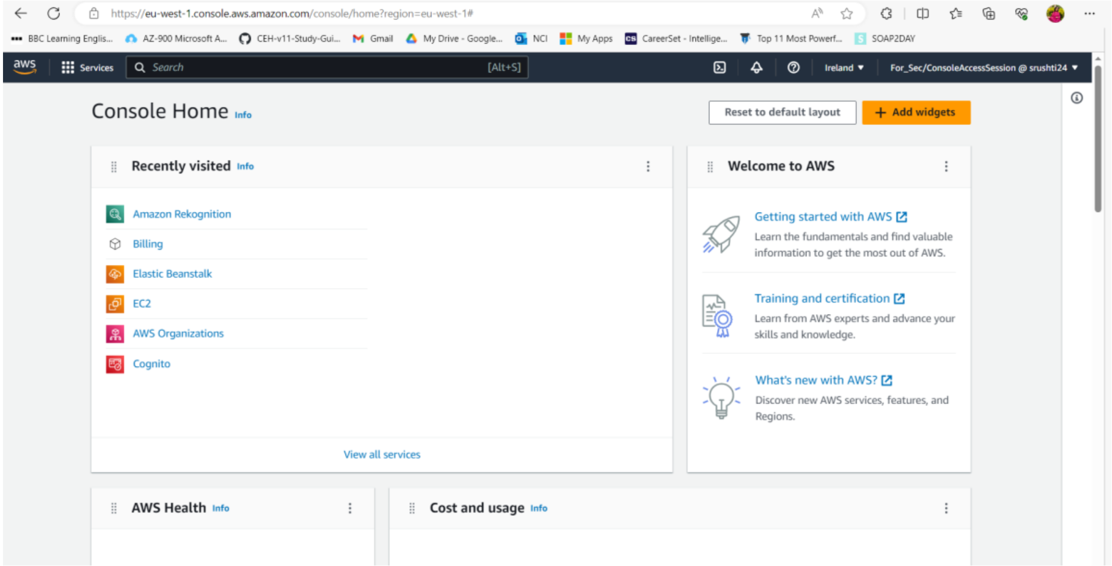
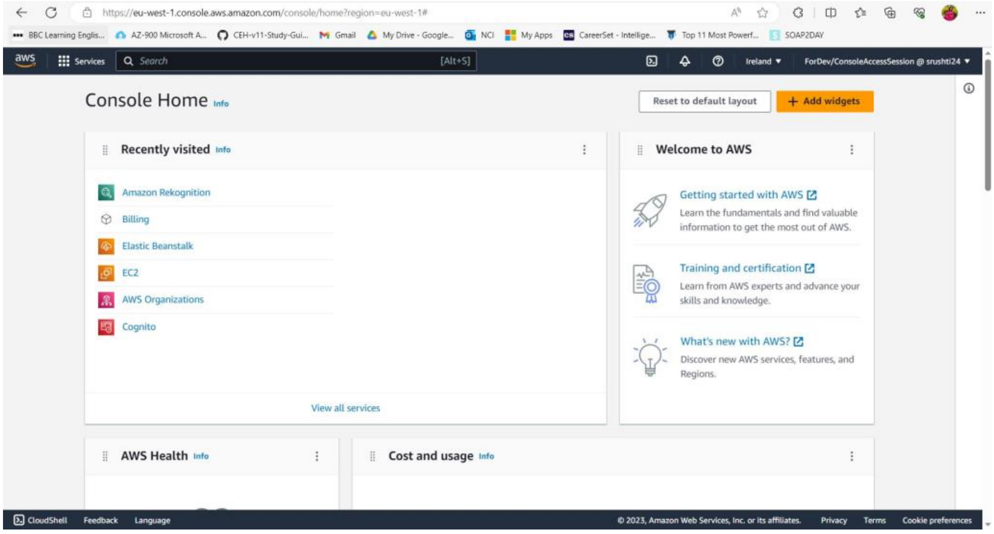

https://eu-west-1.console.aws.amazon.com/console/home?region=eu-west-1#
Services
Search
[Alt+S]
Ireland
For_Sec/ConsoleAccessSession @ srushti24
Console Home Info
Reset to default layout
+ Add widgets
Recently visited Info
Amazon Rekognition
Billing
Elastic Beanstalk
EC2
AWS Organizations
Cognito
View all services
Welcome to AWS
Getting started with AWS
Learn the fundamentals and find valuable information to get the most out of AWS.
Training and certification
Learn from AWS experts and advance your skills and knowledge.
What's new with AWS?
Discover new AWS services, features, and Regions.
AWS Health Info
Cost and usage Info

Figure 9. RBAC role 2



https://eu-west-1.console.aws.amazon.com/console/home?region=eu-west-1#
BBC Learning Englis... AZ-900 Microsoft A... CEH-v11-Study-Gui... Gmail My Drive - Google... NCI My Apps CareerSet - Intellige... Top 11 Most Powerf... SOAP2DAY
aws Services Search [Alt+S]
Ireland
ForDev/ConsoleAccessSession @ srushti24
Reset to default layout
+ Add widgets
View all services
CloudShell Feedback Language
© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Console Home Info

Recently visited Info

- Amazon Rekognition
- Billing
- Elastic Beanstalk
- EC2
- AWS Organizations
- Cognito

Welcome to AWS

Getting started with AWS
Learn the fundamentals and find valuable information to get the most out of AWS.

Training and certification
Learn from AWS experts and advance your skills and knowledge.

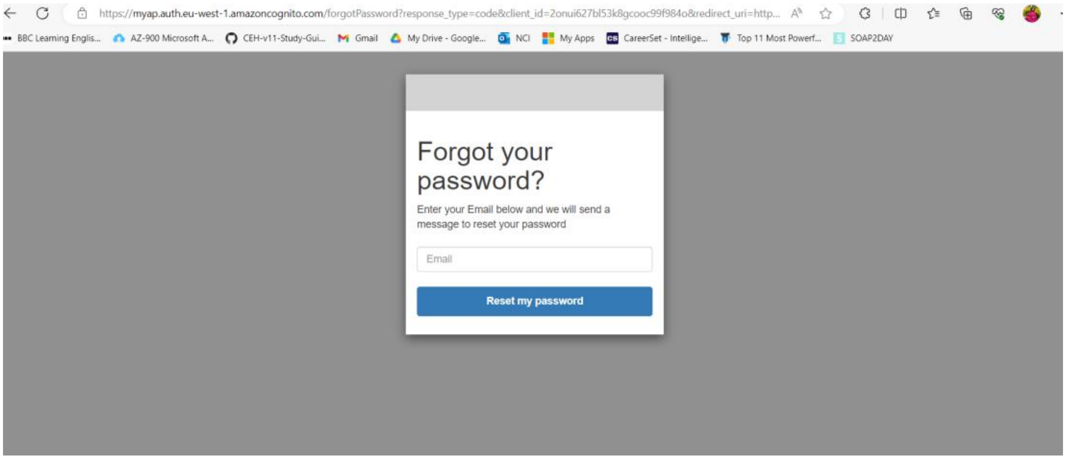
What's new with AWS?
Discover new AWS services, features, and Regions.

AWS Health Info

Cost and usage Info

Figure 10. RBAC role 1

6.5 Test case 5 - Password recovery through email in case of password forget condition (default service provided by AWS Cognito).



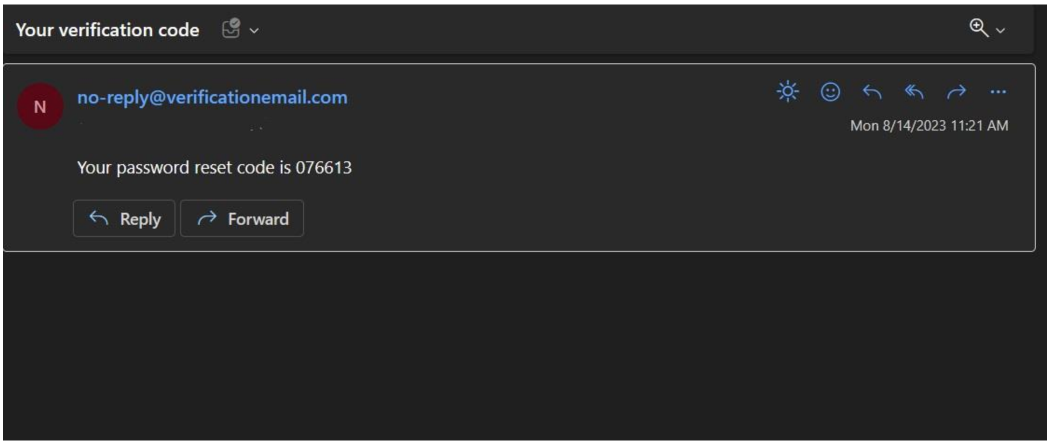
https://myap.auth.eu-west-1.amazoncognito.com/forgotPassword?response_type=code&client_id=2onui627bl53k8gcooc99f984o&redirect_uri=http...
BBC Learning Englis... AZ-900 Microsoft A... CEH-v11-Study-Gui... Gmail My Drive - Google... NCI My Apps CareerSet - Intellige... Top 11 Most Powerf... SOAP2DAY
Reset my password

Forgot your password?

Enter your Email below and we will send a message to reset your password

Email

Figure 11. Password recovery



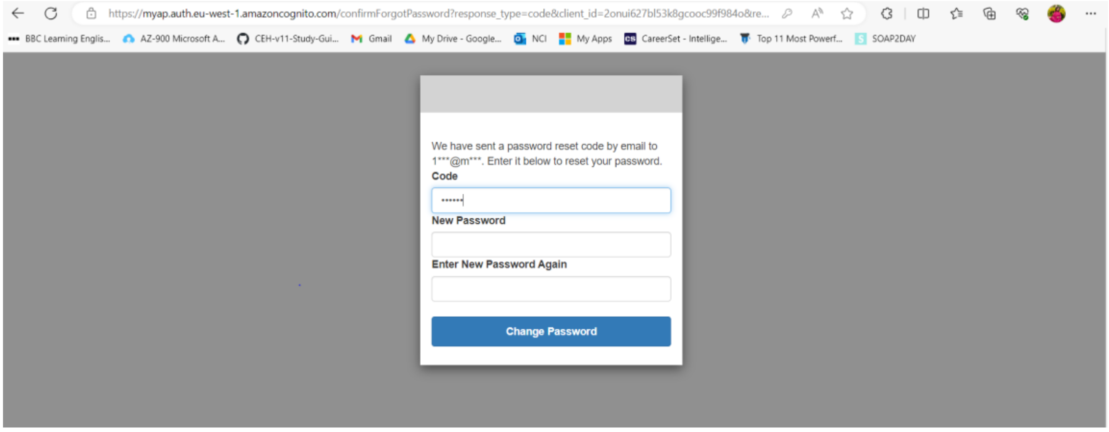
Your verification code

no-reply@verificationemail.com

Mon 8/14/2023 11:21 AM

Your password reset code is 076613

Figure 12. code received on email



https://myap.auth.eu-west-1.amazoncognito.com/confirmForgotPassword?response_type=code&client_id=2onui627bl53k8gcooc99f984o&re...

We have sent a password reset code by email to 1***@m***. Enter it below to reset your password.

Code: ••••••

New Password

Enter New Password Again

Figure 13. Password recovery code

7 Conclusion and Future Work

The multilayered security approach for web application on Amazon web service concludes that we can build robust security mechanism for cloud resources by implementing two different types of multifactor authentication normal role and elevated role and differentiating roles of users. The above implemented mechanism ensures ease of operation as well. The building of this strategy is also simple and straightforward due to flexibility of the AWS services and adaptable integration between AWS services. Hence, we can say that services provided by AWS ecosystem are helpful in meeting security requirements where AWS services are providing security for AWS resources. Applying Biometric authentication layer for the users having higher level of access guarantees reduce in vulnerabilities. The design implementation minimizes the potential points of failures. This approach adapts security principle like least privilege and separation of duties.

For future studies, according to business requirement, customized authentication can be designed with help of AWS Cognito which give vast range of API. Face recognition can be replaced by fingerprint or iris recognition which prove more uniqueness. AWS Cognito can be integrated AWS lambda functions where we can set up lambda trigger. It follows custom authentication level with help of auth challenge API so that no is required to rely on external supply of biometric factor such as third-party authenticator. The overall structure provides better cost management. The further research also can be carried out on IAM policies where we can write customized JSON format which provides resource level access control for AWS users. In future, with successful authentication and authorization process, when user proves identity, redirect tokens towards AWS console can be integrated with AWS SSO service if there is need of access for longer time. This can be done on organization level. Overall, this multilayered sets up benchmark for cloud resource level security.

References

Althamary, I.A. and EL-Alfy, E.-S.M. (2017). *A More Secure Scheme for CAPTCHA-Based Authentication in Cloud Environment*.

Amazon (2019). *AWS Documentation*. [online] Amazon.com. Available at: https://docs.aws.amazon.com/.

aws.amazon.com. (2022). *AWS Named as a Leader in the 2022 Gartner Cloud Infrastructure & Platform Services (CIPS) Magic Quadrant for the 12th Consecutive Year | AWS News Blog*. [online] Available at: https://aws.amazon.com/blogs/aws/aws-named-as-a-leader-in-the-2022-gartner-cloud-infrastructure-platform-services-cips-magic-quadrant-for-the-12th-consecutive-year/.

Gupta, S., Sonkar, P., Papneja, P. and Sharma, M. (2022). Facial Recognition Software Package AWS Rekognition. *Journal of Pharmaceutical Negative Results* ¦, 13. doi:https://doi.org/10.47750/pnr.2022.13.S10.456.

Kadlec, J., Jaros, D. and Kuchta, R. (2010). Implementation of an Advanced Authentication Method within Microsoft Active Directory Network Services. *2010 6th International Conference on Wireless and Mobile Communications*. doi:https://doi.org/10.1109/icwmc.2010.48.

Kaushik, T. (2021). *Implementing an IDaaS for Microsoft Active Directory using SensiPass Three- factor Dynamic Digital Signature MSc Research project Cybersecurity Tushar Kaushik Student ID: 19236158 School of Computing National College of Ireland*.

Kern, A. and Anderl, R. (2018). *Using RBAC to Enforce the Principle of Least Privilege in Industrial Remote Maintenance Sessions*.

Lysakov, V., Sievierinov, O. and Taran, I. (2021). Security of Web Applications Using AWS Cloud Provider. *COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES KHARKIV*. doi:https://doi.org/10.30837/csitic52021232170.

Pinki, Dhiman, H., Hussain, S. and Tech, M. (2014). *A Survey on Identity and Access Management in Cloud Computing*.

Sailakshmi, V. (2021). *Analysis of Cloud Security Controls in AWS, Azure, and Google Cloud*. p.112.

SINGH, C. and SINGH, T.D. (2019). A 3-LEVEL MULTIFACTOR AUTHENTICATION SCHEME FOR CLOUD COMPUTING. *INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING & TECHNOLOGY*, 10(1). doi:https://doi.org/10.34218/ijcet.10.1.2019.020.

Wei Li, Haishan Wan, Xunyi Ren and Sheng Li (2012). A Refined RBAC Model for Cloud Computing. *2012 IEEE/ACIS 11th International Conference on Computer and Information Science*. doi:https://doi.org/10.1109/icis.2012.13.

Wu, R., Zhang, X., Ahn, G.-J., Sharifi, H. and Xie, H. (2013). ACaaS: Access Control as a Service for IaaS Cloud. *2013 International Conference on Social Computing*. doi:https://doi.org/10.1109/socialcom.2013.66.