

A LONG TERM INTERNSHIP REPORT on AMAZON WEB SERVICES

**Submitted to Department of
Computer Science**

BY

T.TEJASWI

3-BCA-B

**Under the Esteemed Guidance of MOUNIKA
lecturer**

Department of Computer Applications



ADITYA DEGREE COLLEGE

VISAKHAPATNAM

ADITYA DEGREE COLLEGE

Department of Computer Applications



CERTIFICATE

This is to certify that The Long Term Internship entitled,

<Amazon Web Services= is a bonified work of T.Tejaswi,
bearing 122127206146, III BCA, submitted to the
Department of Computer Science, Aditya Degree College,
Visakhapatnam for the academic year 2022-2025.

Head of the Department

Sri. A.CHANDRASEKHAR (M.Sc)

External Examiner

Principal

ADITYA DEGREE COLLEGE

Department of Computer Applications



DECLARATION BY THE STUDENT

I hereby declare that the work described in this Long Term Internship, entitled <Amazon Web Services= which is being submitted by me in partial fulfilment of the requirements for the award of degree of Bachelor of Computer Applications(BCA) from the Department of Computer Application to Aditya Degree College, Visakhapatnam under the guidance of Ms.Mounika ,Project Coordinator of Adhoc Network Tech Company,India and Canada.

Place: Visakhapatnam

Date:

ADITYA DEGREE COLLEGE

Department of Computer Applications



CERTIFICATE FROM THE SUPERVISOR

This is to certify that the Long Term Internship entitled, =**AmazonWebServices**=, that is being submitted by **T.Tejaswi** bearing **122127206146,IIIBCA**, which is being submitted by me in partial fulfilment of the requirements for the award of degree of **Bachelor of Computer Applications** from the Bachelor of Computer Applications to Aditya Degree College, bonified work carried out by him under my guidance and Supervision.

Mr.A.Chandra Sekhar(M.sc)

ACKNOWLEDGEMENT

No endeavour is completed without the valuable support of others. I would like to take this opportunity to extend my sincere gratitude to all those who have contributed to the successful completion of this Long-Term Internship Project Report.

It is a privilege to thank **Dr.N.SESHA REDDY, Chairman Sir**, Aditya group of institutions for providing state-of-the-Art facilities, experienced and talented faculty members.

It is a privilege to thank **Dr. N. SUGUNA REDDY, Secretary Madam**, Aditya group of institutions for providing Long-Term Internship Project Report from Adhoc.

I thank **Dr.B.E.V.L.Naidu Sir**, Academic Director, Aditya Degree College for his continuous support and encouragement in my endeavour.

I sincerely extend my heartfelt gratitude to **CEngg Daniel Benjamin Sir, Chartered Engineer, AMIE, B.Tech**, Project Director of Adhoc Network Tech Company, India and Canada, for his invaluable guidance, timely support, and insightful contributions through his dedicated company team. His expertise and leadership have been instrumental in the successful completion of my Long-Term Internship Project Report.

At this juncture I feel deeply honoured in expressing my sincere thanks to **CEO Devika Pakruthi Mam** of Adhoc Network Tech Company, India and Canada for making the resources available at the right time and providing valuable insights leading to the successful completion of my Long-Term Internship Project Report.

I express my deep sense of gratitude to **Mr. Shahid Ali(M.Sc, PhD), Principal**, for his efforts and for giving us permission for carrying out this Long-Term Internship.

I thank **Mr.A.Chandra Sekhar, M.Sc** Head of the Department of Bachelor of Computer Science, Aditya Degree College- Visakhapatnam, for supporting and encouraging me in completion of my Long-Term Internship.

Finally I thank all the faculty members of our Department who contributed their valuable suggestions in completion of Long-Term Internship report and I also put my sincere thanks to My Parents who stood with me during the whole Long-Term Internship.

ABOUT ADITYA DEGREE COLLEGES



Dr.N.SESHA REDDY
CHAIRMAN



Dr. N. Suguna Reddy M.B.B.S. Secretary



Dr.B.E.V.L. NAIDU
ACADEMIC DIRECTOR

Aditya Degree colleges are the precious gifts presented to the twin Godavari Districts by ADITYA Educational group. ADITYA Degree College which was established in 1998 in Kakinada fulfilled the hopes and aspirations of many graduates and had been acclaimed as the best degree college under Andhra University. Encouraged by the 100% result in 2003, ADITYA added several feathers to its cap by launching Degree Colleges in Rajahmundry in 2003, in Vizag and Palakollu in 2005 and in Tatipaka in 2006.

Needless to say, in the present scenario girls excel more than boys in education and they give tough competition to boys. Owing to their indifference and inhibition, girls find difficulty in expressing their doubts in a classroom of Co-ed College. Moreover, parents have many objections in sending their daughters to a co-ed college. Realizing this, ADITYA successfully leads Degree colleges for girls to prove their talents in curricular, co-curricular and extra-curricular activities. ADITYA started P.G College also for Women to encourage them for higher education.

VISION

To provide inclusive education with innovative methods and strenuous efforts for inculcating human values, professionalism and scientific instillation in the realm of Degree Education to all sections of students irrespective of race, region and religion with special focus to stand independently and to emerge as centre for Research and Development.

MISSION

To provide ample scope for multifaceted development of local youth. To provide quality higher education to student community. To Recruit Highly Qualified and Experienced Faculty to provide Quality Education.

ABOUT ADHOC NETWORK TECH COMPANY - INDIA,CANADA



CEO Devika Pakruthi is a highly accomplished and recognized entrepreneur who has garnered prestigious awards at various levels for her outstanding contributions to the business world.

Awards that Devika Pakruthi has won:

- Young Entrepreneur Award - City Level (Visakhapatnam)
- Best Ongoing Startup - State Level (Andhra Pradesh)
- Women Rising Star of the Year- National Level (New Delhi)
- Youngest CEO of the Year - State Representation (Karnataka)

AdhocNetworkisstartedintheyear2020at Visakhapatnam byanyoungWomenentrepreneur Miss.DevikaPakruthi Founder&CEOwithan intentionto provideemploymentopportunitiesto theyouthandalsoto impartthebestquality training andpracticalexposureto theStudentswhich enhancestheiremployability Skills. Herjourney startedand collapsedwiththewidespreadofCovid-19buther determinationandaspirationsmadeher journeymore futuristicandshenevergaveupthe thoughtto GIVE-UP. This iswhereDevikamadeher dreamscometrueandalive. She neverexpectedwith asole objectiveofmakingProfitbuther determinationto impartthequalitytrainingmadeher to reachthepeaksofsuccessattheyoungage.

Adhoc Network-we are proud to have been awarded a Hattrick of Awards. This Achievement is a testament to our commitment to Excellence and Innovation in the Software development Best heading company in the market. Devika Pakruthi, a name synonymous with innovation, empowerment, and success. As the proud recipient of the Young Entrepreneur Award, Best Women-Led Startup Award, Women Rising Star of the Year Award and Youngest CEO of the Year Award, Devika Pakruthi has etched her name into the annals of contemporary business history.

Vision, Mission and values of the Organization:-

VISION:- Due vision is to be a leading global provider of interactive and reliable Software Solution empowering business to Thrive in the digital age.

MISSION:- Our mission is to develop cutting-edge Software Solutions that Solve compare business challenges, enhance Operations efficiency and drive Sustainable growth for our client we strive to deliver exceptional value by leveraging emerging technologies, fostering Strategic partnerships and maintaining a Customer, Centric approach Values

- Innovation
- Excellence
- Collaboration
- Integrity
- Customer Centricity
- Continuous Learning



ADHOC NETWORK

CERTIFICATE OF INTERNSHIP

This Certificate is Presented To :

TEJASWI TADELU

From demonstrated exceptional dedication and commitment to mastering AWS CC Internship actively engaging in hands-on projects and practical learning from **December 5th 2024-March 15th-2025**. Your active participation and engagement in the Internship have equipped you with valuable technical skills and practical knowledge essential for building dynamic and scalable applications



TECHNICAL TRAINER

ABSTRACT

Cloud storage has become a popular option for storing and managing large amounts of data due to its convenience, scalability, and cost-effectiveness. However, the security and privacy of cloud-stored data remain a significant concern. Encrypting data before uploading it to the cloud is a common solution to address these concerns. However, searching over encrypted data is a challenging problem, particularly when there are multiple keywords involved. While many of the currently available ranked keyword search schemes aim to improve search efficiency or functionality, they often fail to provide both efficient access control and rigorous security analysis at the same time. This creates a gap in the available security and privacy options for such systems. To address these limitations, this paper presents a novel solution called the Multi-keyword Ranked Search scheme with Fine-grained access control (MRSF). MRSF is designed to offer both efficient and privacy-preserving search capabilities, as well as robust access control measures. This allows for highly accurate retrieval of encrypted data, while also ensuring that only authorized users are able to access it. This project proposes a practical multi-keyword ranked search with access control scheme for encrypted cloud data. The proposed scheme allows data owners to encrypt their data and upload it to the cloud while maintaining the ability to search over the data without compromising its security. The scheme also provides access control to ensure that only authorized users can access the data. The proposed scheme uses a combination of symmetric and asymmetric encryption to enable efficient multi-keyword search over the encrypted data. The scheme employs an index-based search mechanism to achieve a ranked search based on the relevance of the keywords. The access control is implemented using attribute-based encryption, which allows access to be granted or revoked based on specific attributes of the user. Experimental evaluations demonstrate the effectiveness and efficiency of the proposed scheme, making it a viable solution for practical multi-keyword search with access control over encrypted cloud data. This project contributes to the field of cloud security and privacy by providing a practical solution to address the challenges of searching over encrypted cloud data while maintaining its security and privacy.

INDEX

S.NO	CONTENTS	PAGE NO
1	Create an Aws Account	
2	Design a computer lab using a router & Switch	
3	Design a computer lab using a router & Switch	
4	Aws Console Services.	
5	Aws global infra-Structure	
6	Create a false storage Dropbox	
7	Create an I Am user account	
8	Create a group in IAM	
9	Create Alias for your AWS Account	
10	login to IAM user.	
11	Create IAM policy inheritance for your company.	
12	Remove the permission for a specific user in IAM	
13	I Am password policy	
14	Login using MFA Code	
15	Elastic compute cloud (EC2)	
16	Creation of S3 bucket and objects	
17	Mini Project-1	
18	Mini Project-2	
19	Major Project	

INTRODUCTION

What is cloud computing?

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third- party services. These services typically provide access to advanced software applications and high-end networks of server computers.

Structure of cloud computing

How Cloud Computing Works?

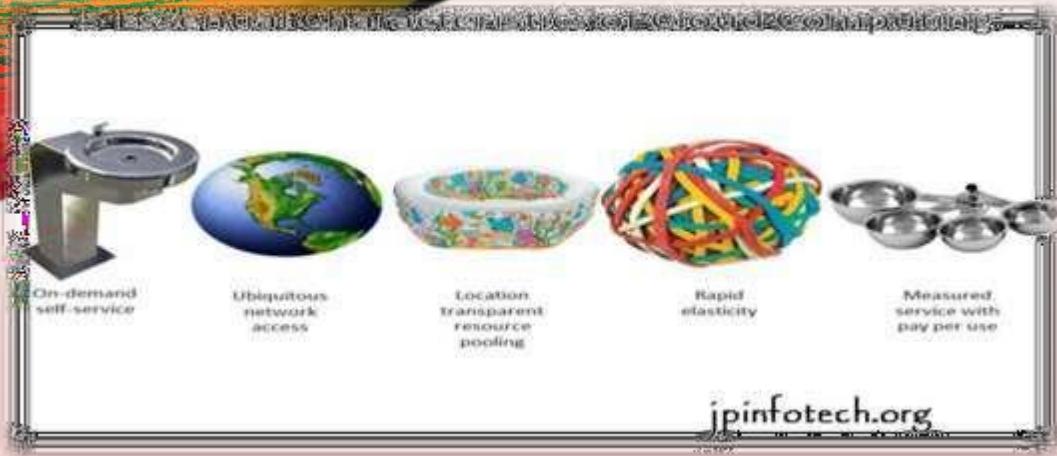
The goal of cloud computing is to apply traditional supercomputing, or high- performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data- processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

Characteristics and Services Models:

The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

- **On-demand self-service:** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- **Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- **Resource pooling:** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- **Rapid elasticity:** Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- **Measured service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.



Characteristics of cloud computing

Services Models: Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. The model is shown in figure below. If a cloud user accesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If she accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider.

Structure of service models

Benefits of cloud computing:

1. **Achieve economies of scale – increase volume output or productivity with fewer people. Your cost per unit, project or product plummets.**
2. **Reduce spending on technology infrastructure. Maintain easy access to your information with minimal upfront spending. Pay as you go (weekly, quarterly or yearly), based on demand.**
3. **Globalize your workforce on the cheap. People worldwide can access the cloud, provided they have an Internet connection.**
4. **Streamline processes.** Get more work done in less time with less people.
5. **Reduce capital costs.** There's no need to spend big money on hardware, software or licensing fees.
6. **Improve accessibility.** You have access anytime, anywhere, making your life so much easier!

1. Monitor projects more effectively. Stay within budget and ahead of completion cycle times.
2. Less personnel training is needed. It takes fewer people to do more work on a cloud, with a minimal learning curve on hardware and software issues.
3. Minimize licensing new software. Stretch and grow without the need to buy expensive software licenses or programs.
4. Improve flexibility. You can change direction without serious "people" or "financial" issues at stake.

11. Advantages:

1. Price: Pay for only the resources used.
2. Security: Cloud instances are isolated in the network from other instances for improved security.
3. Performance: Instances can be added instantly for improved performance. Clients have access to the total resources of the Cloud's core hardware.
4. Scalability: Auto-deploy cloud instances when needed.
5. Uptime: Uses multiple servers for maximum redundancies. In case of server failure, instances can be automatically created on another server.
6. Control: Able to login from any location. Server snapshot and a software library lets you deploy custom instances.
7. Traffic: Deals with spike in traffic with quick deployment of additional instances to handle the load.

LITERATURE SURVEY

1. Secure ranked keyword search over encrypted cloud data AUTHORS: C. Wang, N. Cao, J. Li, K. Ren, and W. Lou

As Cloud Computing becomes prevalent, sensitive information are being increasingly centralized into the cloud. For the protection of data privacy, sensitive data has to be encrypted before outsourcing, which makes effective data utilization a very challenging task. Although traditional searchable encryption schemes allow users to securely search over encrypted data through keywords, these techniques support only boolean search, without capturing any relevance of data files.

This approach suffers from two main drawbacks when directly applied in the context of Cloud Computing. On the one hand, users, who do not necessarily have pre- knowledge of the encrypted cloud data, have to postprocess every retrieved file in order to find ones most matching their interest; On the other hand, invariably retrieving all files containing the queried keyword further incurs unnecessary network traffic, which is absolutely undesirable in today's pay-as-you- use cloud paradigm. In this paper, for the first time we define and solve the problem of effective yet secure ranked keyword search over encrypted cloud data. Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency), thus making one step closer towards practical deployment of privacy-preserving data hosting services in Cloud Computing. We first give a straightforward yet ideal construction of ranked keyword search under the state-of-the-art searchable symmetric encryption (SSE) security definition, and demonstrate its inefficiency. To achieve more practical performance, we then propose a definition for ranked searchable symmetric encryption, and give an efficient design by properly utilizing the existing cryptographic primitive, order-preserving symmetric encryption (OPSE). Thorough analysis shows that our proposed solution enjoys "as-strong- aspossible" security guarantee compared to previous SSE schemes, while correctly realizing the goal of ranked keyword search. Extensive experimental results demonstrate the efficiency of the proposed solution.

2. Privacy-preserving and dynamic multi-attribute conjunctive keyword search over encrypted cloud data

AUTHORS: L. Zhang, Y. Zhang, and H. Ma

With the increasing popularity of cloud computing, a growing data owners are motivated to outsource their huge data to cloud servers in order to facilitate access and save data management cost. To protect user privacy and data security, sensitive data should be encrypted before outsourced to the cloud server, which obsoletes data utilization like efficient search over encrypted data. In this paper, we present a privacy-preserving conjunctive keyword search scheme over encrypted cloud data, which simultaneously supports dynamic update operations. Specifically, we construct an index structure based on Multi-Attribute Tree (MAT) and present an efficient search algorithm over the index tree, named as thesearchMAT algorithm. We propose a multi-attribute conjunctive keyword search scheme based on MAT,

named as the MCKS-MAT scheme, which can achieve equality conjunction, subset conjunction and range conjunction, as well as satisfy privacy requirements under the known background attack model. In addition, this paper is accompanied by an adequate of experiments for evaluating the effectiveness of the proposed scheme. Experiments demonstrate that, compared to the linear search, the proposed scheme needs the slightly higher preprocessing cost on account of constructing the tree-based index, however, it achieves lower computational overhead in initialization, trapdoor generation and queries. OAPA

3. Privacy-preserving multi-keyword ranked search over encrypted cloud data

AUTHORS: N. Cao, C. Wang, M. Li, K. Ren, and W. Lou,

With the advent of cloud computing, data owners are motivated to outsource their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings. But for protecting data privacy, sensitive data have to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted cloud data search service is of paramount importance. Considering the large number of data users and documents in the cloud, it is necessary to allow multiple keywords in the search request and return documents in the order of their relevance to these keywords. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely sort the search results. In this paper, for the first time, we define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing (MRSE). We establish a set of strict privacy requirements for such a secure cloud data utilization system. Among various multi-keyword semantics, we choose the efficient similarity measure of "coordinate matching," i.e., as many matches as possible, to capture the relevance of data documents to the search query. We further use "inner product similarity" to quantitatively evaluate such similarity measure. We first propose a basic idea for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. To improve search experience of the data search service, we further extend these two schemes to support more

search semantics. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given.

Experiments on the real-world data set further show proposed schemes indeed introduce low overhead on computation and communication.

4. Practical techniques for searches on encrypted data AUTHORS: D. X. Song, D. Wagner, and A. Perrig

It is desirable to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. For example, if a client wishes to retrieve only documents containing certain words, it was not previously known how to let the data storage server perform the search and answer the query, without loss of data confidentiality. We describe our cryptographic schemes for the problem of searching on encrypted data and provide proofs of security for the resulting crypto systems. Our techniques have a number of crucial advantages. They are provably secure: they provide provable secrecy for encryption, in the sense that the untrusted server cannot learn anything about the plaintext when only given the ciphertext; they provide query isolation for searches, meaning that the untrusted server cannot learn anything more about the plaintext than the search result; they provide controlled searching, so that the untrusted server cannot search for an arbitrary word without the user's authorization; they also support hidden queries, so that the user may ask the untrusted server to search for a secret word without revealing the word to the server. The algorithms presented are simple, fast (for a document of length n , the encryption and search algorithms only need $O(n)$ stream cipher and block cipher operations), and introduce almost no space and communication overhead, and hence are practical to use today

5. Privacy preserving keyword searches on remote encrypted data, AUTHORS: Y.-C. Chang and M. Mitzenmacher

We consider the following problem: a user U wants to store his files in an encrypted form on a remote file server S . Later the user U wants to efficiently retrieve some of the encrypted files containing (or indexed by) specific keywords, keeping the keywords themselves secret and not jeopardizing the security of the remotely stored files. For example, a user may want to store old e-mail messages encrypted on a server managed by Yahoo or another large vendor, and later retrieve certain messages while travelling with a mobile device. In this paper, we offer solutions for this problem under well-defined security requirements. Our schemes are efficient in the sense that no public-key cryptosystem is involved. Indeed, our approach is independent of the encryption method chosen for the remote files. They are also incremental, in that U can submit new files which are secure against previous queries but still searchable against future queries.

SYSTEM STUDY

FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates.

During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are:

- **ECONOMICAL FEASIBILITY**
- **TECHNICAL FEASIBILITY**
- **SOCIAL FEASIBILITY**

ECONOMICAL FEASIBILITY

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

SOCIAL FEASIBILITY

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

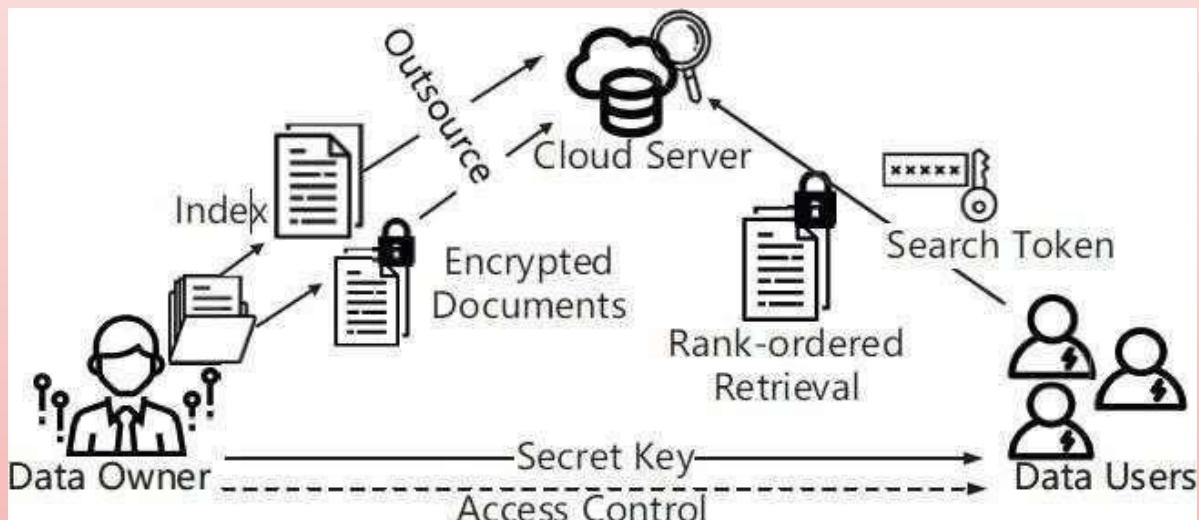
SYSTEM REQUIREMENTS

HARDWARE REQUIREMENTS:

- System : Pentium i3 Processor
- Hard Disk : 500 GB.
- Monitor : 15" LED
- Input Devices : Keyboard, Mouse
- Ram : 2 GB

SYSTEM DESIGN

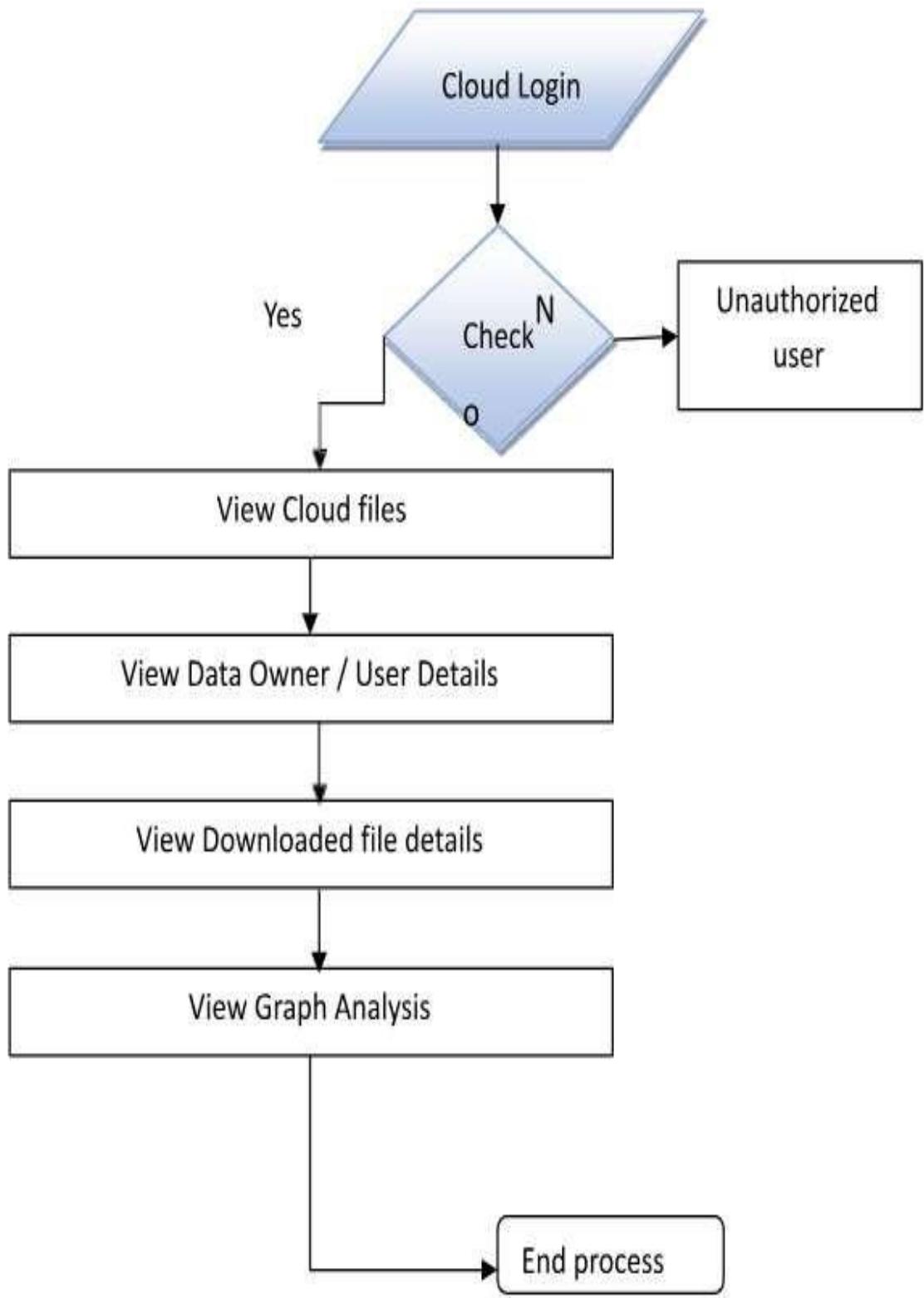
SYSTEM ARCHITECTURE



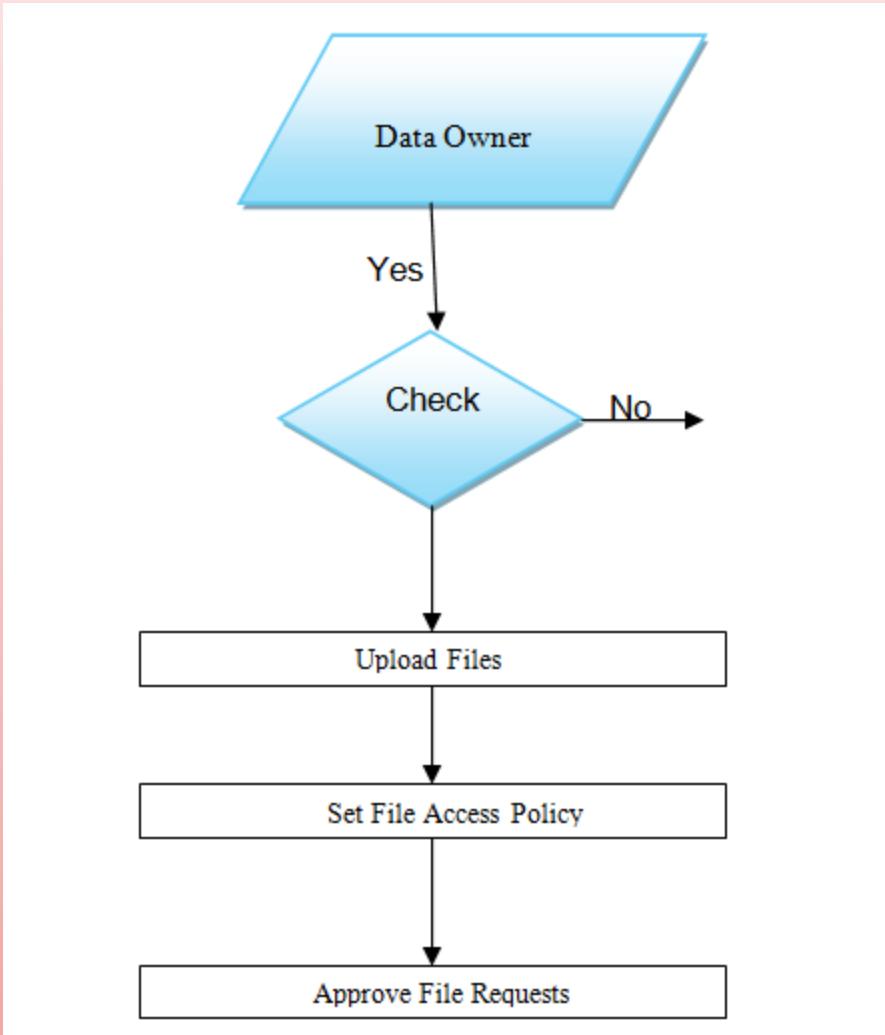
DATA FLOW DIAGRAM:

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

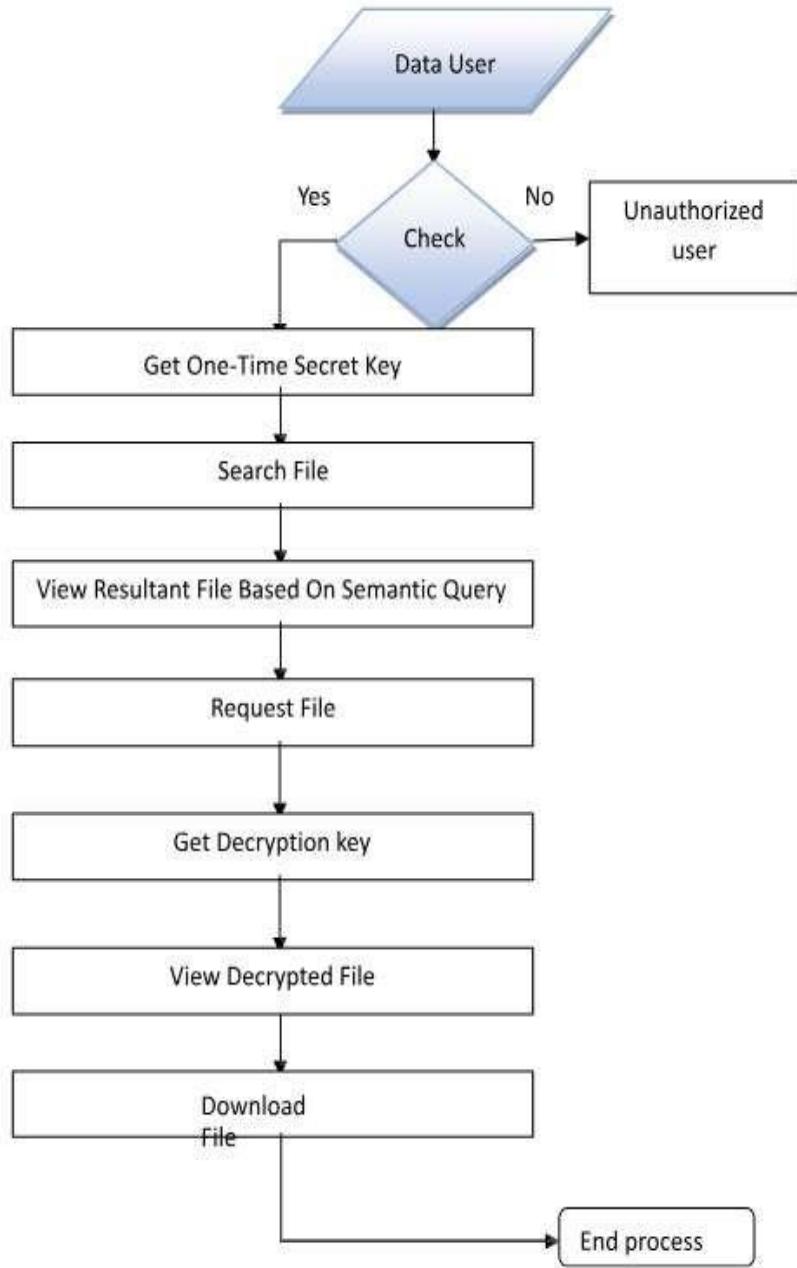
Cloud Server:



Data Owner:



Data User:



UML DIAGRAMS

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group.

The goal is for UML to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems.

The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems.

The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

GOALS:

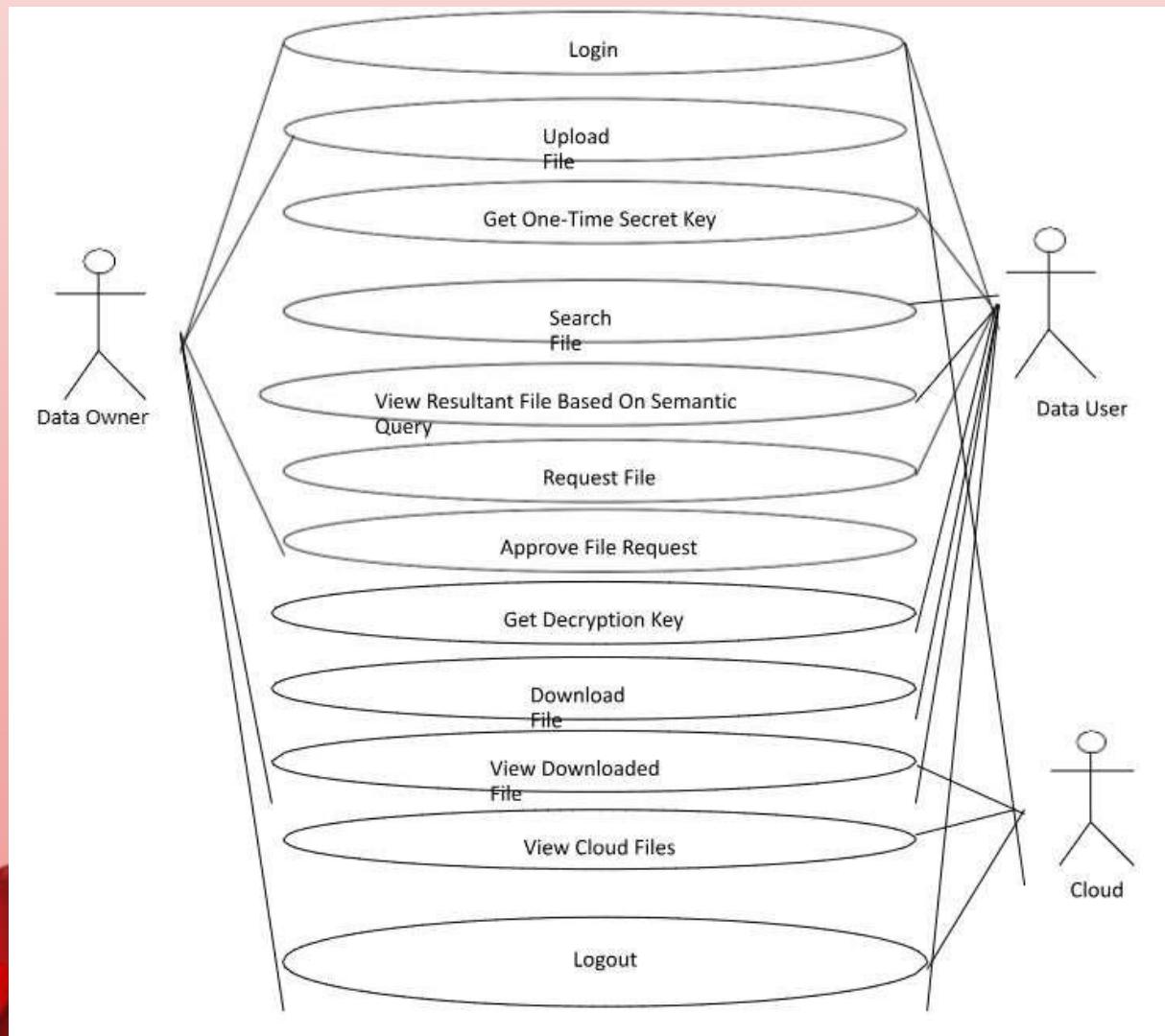
The Primary goals in the design of the UML are as follows:

1. Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.
2. Provide extendibility and specialization mechanisms to extend the core concepts.
3. Be independent of particular programming languages and development process.
4. Provide a formal basis for understanding the modeling language.
5. Encourage the growth of OO tools market.
6. Support higher level development concepts such as collaborations, frameworks, patterns and components.

Integrate best practices

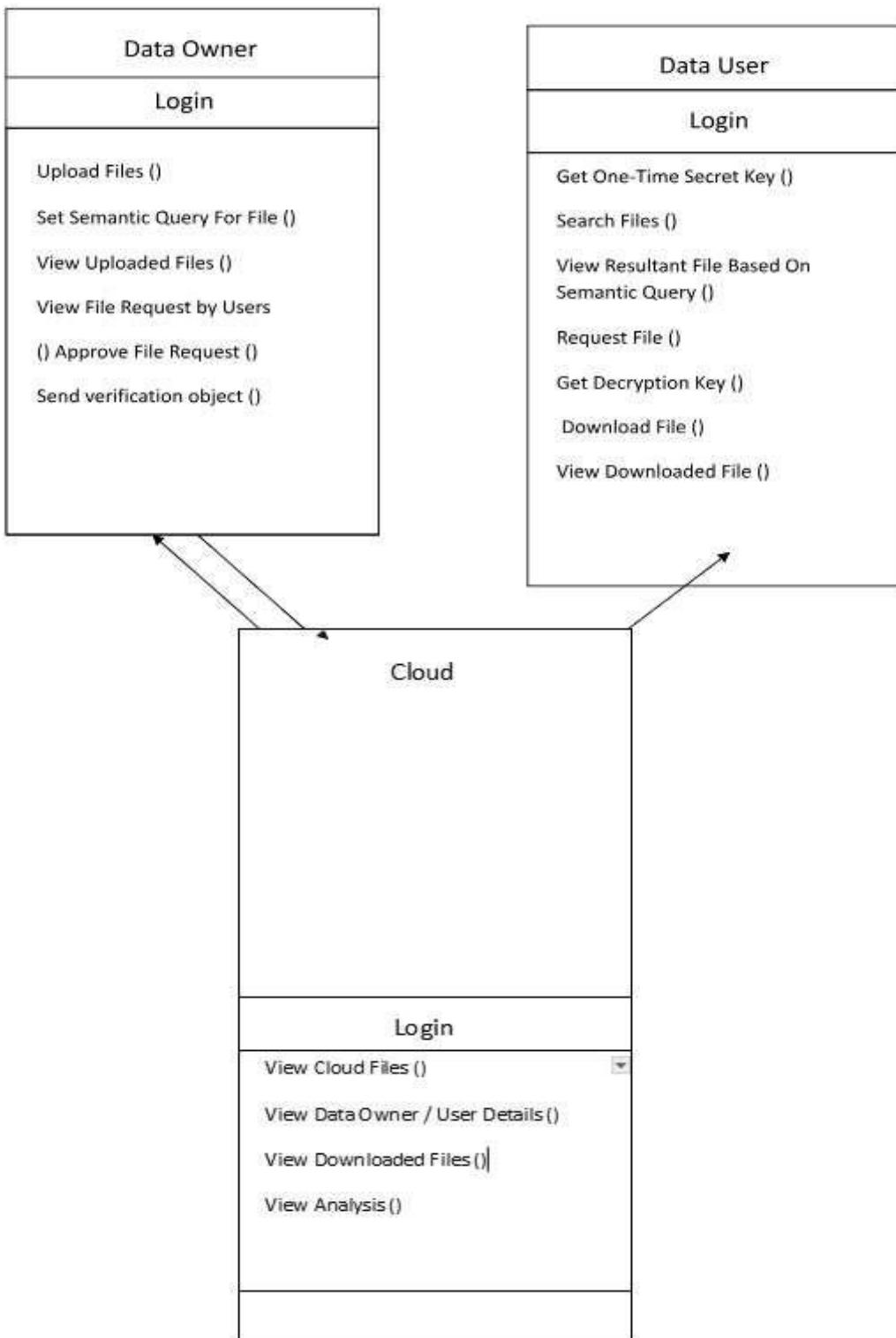
USE CASE DIAGRAM:

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.



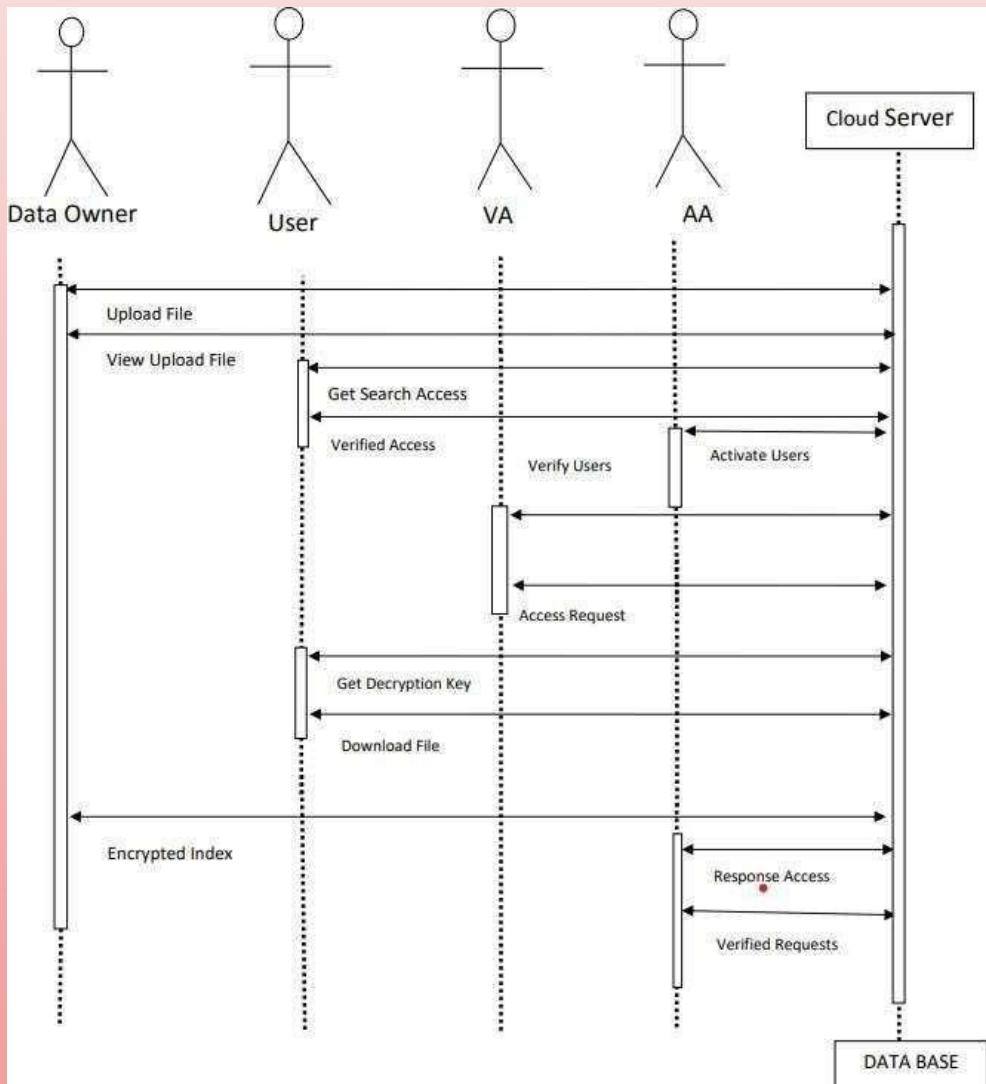
CLASS DIAGRAM:

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.



SEQUENCE DIAGRAM:

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams



ADHOC NETWORKS AWS CLOUD COMPUTING

PROJECT 1

Cloud computing is a technology that enables users to access and use computing resources (such as servers, storage, databases, networking, software, analytics, and intelligence) over the internet ("the cloud") instead of owning and managing physical hardware and infrastructure.

Key Characteristics

On-Demand Self-Service

Broad Network Access

Resource Pooling

Rapid Elasticity

Measured Service

Cloud Service Models

Infrastructure as a Service (IaaS)

Platform as a Service (PaaS)

Software as a Service (SaaS)

Cloud Deployment Models

Public Cloud

Private Cloud

Hybrid Cloud

Major Cloud Service Provider

Amazon Web Services (AWS)

Microsoft Azure

Google Cloud Platform (GCP)

Steps to create an aws account:

Step 1: Visit the aws website.

<https://aws.amazon.com/>

Step 2 : Click on create an aws account.

Step 3 : Sign in or create an amazon account.

Step 4: Provide account info.

Step 5: Contact info, payment info.

Step 6: Identity verification.

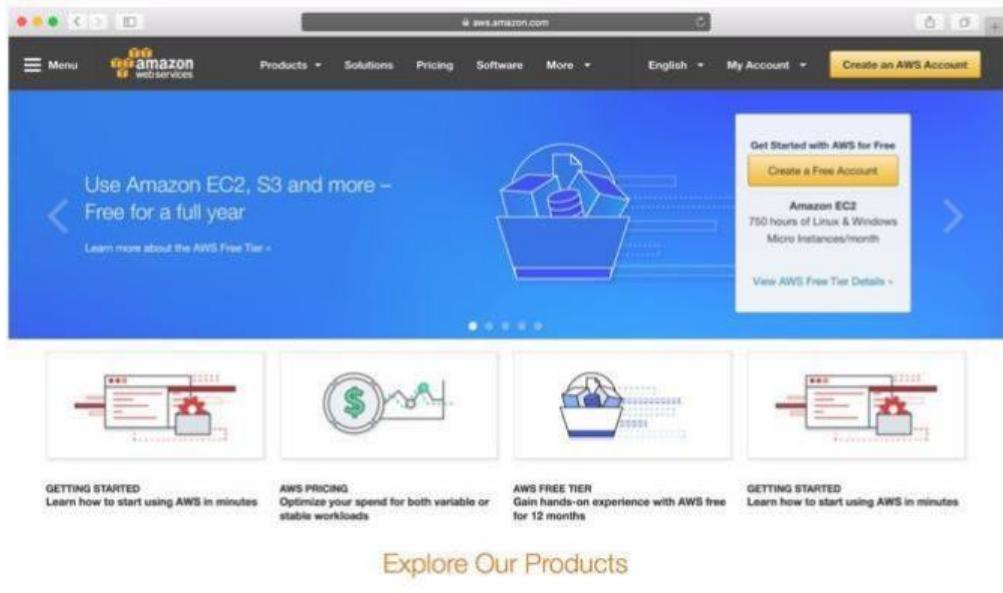
Step 7: Choose a support plan.

Step 8: Review and accept the terms.

Step 9: Confirmation mail.

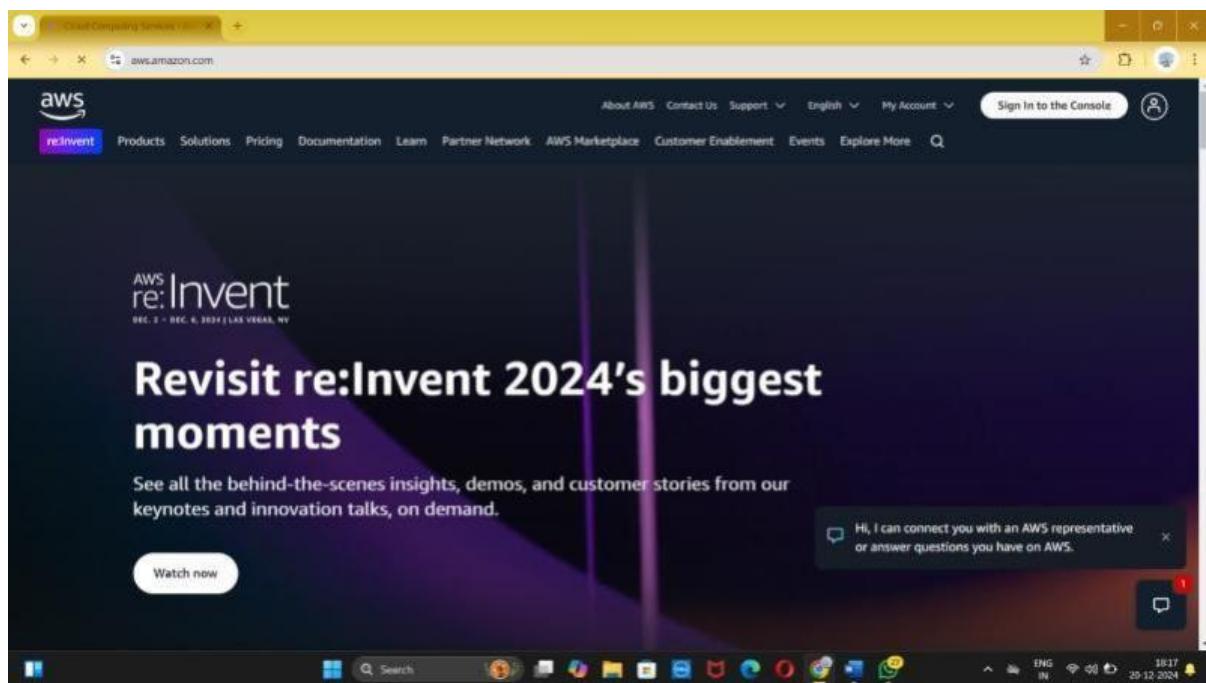
Step 10: Set up aws management console.

Step 11: Explore aws services.



Step 1: Visit the aws website.

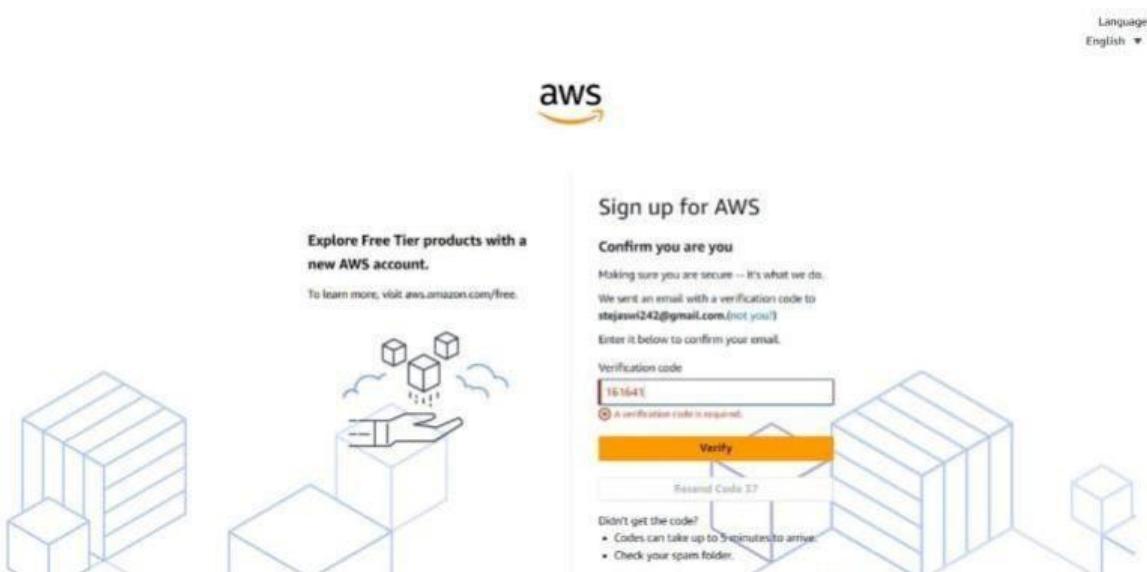
<https://aws.amazon.com/>



Step 2 : Click on create an aws account.



Step 3 : Sign in or create an amazon account.



Step 4: Provide account info.

Explore Free Tier products with a new AWS account.

To learn more, visit aws.amazon.com/free.



Sign up for AWS

Create your password

It's you! Your email address has been successfully verified. X

Your password provides you with sign in access to AWS, so it's important we get it right.

Root user password

Confirm root user password

***** key icon

Continue (step 1 of 5)

OR

Sign in to an existing AWS account

Step 5: Contact info, payment info.

Free Tier offers

All AWS accounts can explore 3 different types of free offers, depending on the product used.



Always free

Never expires



12 months free

Start from initial sign-up date



Trials

Start from service activation date



Sign up for AWS

Contact Information

How do you plan to use AWS?

- Business - for your work, school, or organization
 Personal - for your own projects

Who should we contact about this account?

Full Name

Phone Number

US +1 222-333-4444

Country or Region

United States

Address

Address

City

State, Province, or Region

Postal Code

I have read and agree to the terms of the
[AWS Customer Agreement](#).

Continue (step 2 of 5)



payment info

Secure verification

ⓘ We will not charge you for usage below AWS Free Tier limits. We may temporarily hold up to \$1 USD (or an equivalent amount in local currency) as a pending transaction for 3-5 days to verify your identity.



Sign up for AWS

Billing Information

Credit or Debit card number



AWS accepts most major credit and debit cards. To learn more about payment options, review our [FAQ](#)

Expiration date

Month Year

Security code ⓘ

Cardholder's name

Save card information for faster future payments

Securely save card information payments as per RBI guidelines. [Learn more](#).

Billing address

Use my contact address

1-43-109,Thagarapuvalasa
 Visakhapatnam Andhra Pradesh 531162

aws

Sign up for AWS

Secure verification

We will not charge you for usage below AWS Free Tier limits. We may temporarily hold up to \$1 USD (or an equivalent amount in local currency) as a pending transaction for 3-5 days to verify your identity.



Billing Information

Billing country
Your billing country determines the payment methods available to you to pay for AWS services.

India

Credit or Debit card number
6529654794448640



AWS accepts most major credit and debit cards. To learn more about payment options, review our [FAQ](#).

Expiration date
November 2031

Security code 

Cardholder's name
MUKALLA PRAVEEN KUMAR



Save card information for faster future payments.
Securely save card information payments as per NRI guidelines. [Learn more](#)

Save card information for faster future payments.

Billing address:

Use my contact address
10/3-288, Nehru Nagar, Ramnagar,
Visakhapatnam Andhra Pradesh
530002
IN

Use a new address

Do you have a PAN?
Permanent Account Number (PAN) is a ten-digit alphanumeric identifier issued by the Indian Income Tax Department. This 10-digit number is printed on the front of your PAN card.

Yes

No

You can go on the Tax Settings Page on Billing and Cost Management Console to update your PAN information.

[View and continue to step 7](#)

Step 6: Identity verification.

aws

Sign up for AWS

Confirm your identity India

Primary purpose of account registration
Choose one that best applies to you. If your account is for business, select the one that applies to your business.

Personal use

Ownership type
Choose your ownership relation to the account. Selecting this option may require you to complete additional customer verification steps.

Individual

India document type  India
To verify your identity, the name on the document must match the name that you chose.

PAN card

Date of birth
To use this document type, you must be at least 18 years old.

2003/11/23

Format: YYYY/MM/DD



Choose one that best applies to you. If your account is tied to a business, select the one that applies to your business.

Personal use

Ownership type

Choose your ownership relation to the account.
Based on your selection, you may be asked to complete additional customer verification steps.

Individual

India document type (i) info

To verify your identity, the name on the document must match the name that you chose.

PAN card

Date of birth

To use this document type, you must be at least 18 years old.

2003/11/23

Format: YYYY/MM/DD

Permanent Account Number (PAN)

CRWPT1892A

The PAN is 10 alphanumeric characters without spaces or tabs. Example: AAAAAA1111B

Name (i) info

Choose the name that you want to use for identity verification.

Tejaswi Tadelu

Upload front of Permanent Account

The PAN is 10 alphanumeric characters without spaces or tabs. Example: AAAAAA1111B

Name (i) info

Choose the name that you want to use for identity verification.

Tejaswi Tadelu

Upload front of Permanent Account
Number (PAN) card

Choose file

File must be in .pdf, .jpg, .jpeg, or .png format.
Maximum file size 5 MB.

WhatsApp Image 2024-12-20 at 13.48.52_c1fe1b84.jpg X
62.89 KB

I consent to allowing AWS to use and send the information above to a third-party service for identity verification purposes.

Continue (step 4 of 5)



Sign up for AWS

Confirm your identity



Before you can use your AWS account, you must verify your phone number. When you continue, the AWS automated system will contact you with a verification code.

How should we send you the verification code?

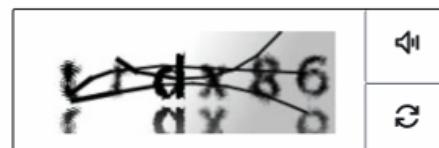
- Text message (SMS)
 Voice call

Country or region code

India (+91) ▾

Mobile phone number

Security check



Type the characters as shown above

Send SMS (step 4 of 5)

The screenshot shows the AWS sign-up process at step 4 of 5, titled "Confirm your identity". It features a CAPTCHA challenge, a verification code input field containing "4584", and a "Continue (step 4 of 5)" button. The AWS logo is visible at the top. The background includes a decorative graphic of 3D cubes.

Sign up for AWS

Confirm your identity

Verify code
4584

Continue (step 4 of 5)

Having trouble? Sometimes it takes up to 10 minutes to retrieve a verification code. If it's been longer than that, return to the previous page and try again.

Privacy Policy | Terms of Use | Cookie Preferences | Sign Out

Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step 7: Choose a support plan.

Sign up for AWS

Select a support plan

Choose a support plan for your business or personal account. [Compare plans and pricing examples](#)  You can change your plan anytime in the AWS Management Console.

Basic support - Free

- Recommended for new users just getting started with AWS
- 24x7 self-service access to AWS resources
- For account and billing issues only
- Access to Personal Health Dashboard & Trusted Advisor



Developer support - From \$29/month

- Recommended for developers experimenting with AWS
- Email access to AWS Support during business hours
- 12 (business)-hour response times



Business support - From \$100/month

- Recommended for running production workloads on AWS
- 24x7 tech support via email, phone, and chat
- 1-hour response times
- Full set of Trusted Advisor best-practice recommendations



Need Enterprise level support?

From \$15,000 a month you will receive 15-minute response times and concierge-style experience with an assigned Technical Account Manager. [Learn more](#) 

[Complete sign up](#)



Congratulations

Thank you for signing up for AWS.

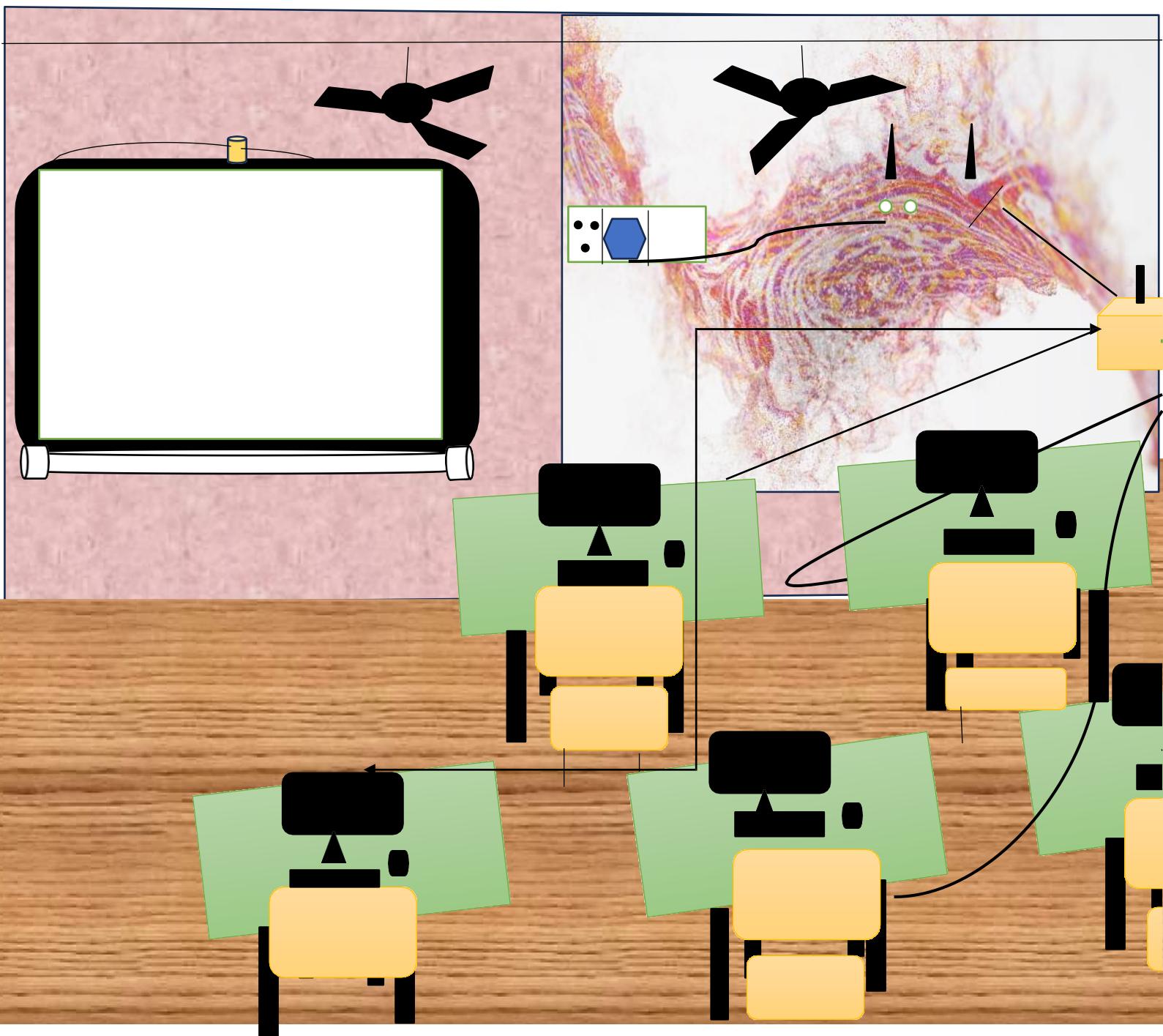
We are activating your account, which should only take a few minutes. You will receive an email when this is complete.

[Go to the AWS Management Console](#)

[Sign up for another account](#) or [contact sales](#).

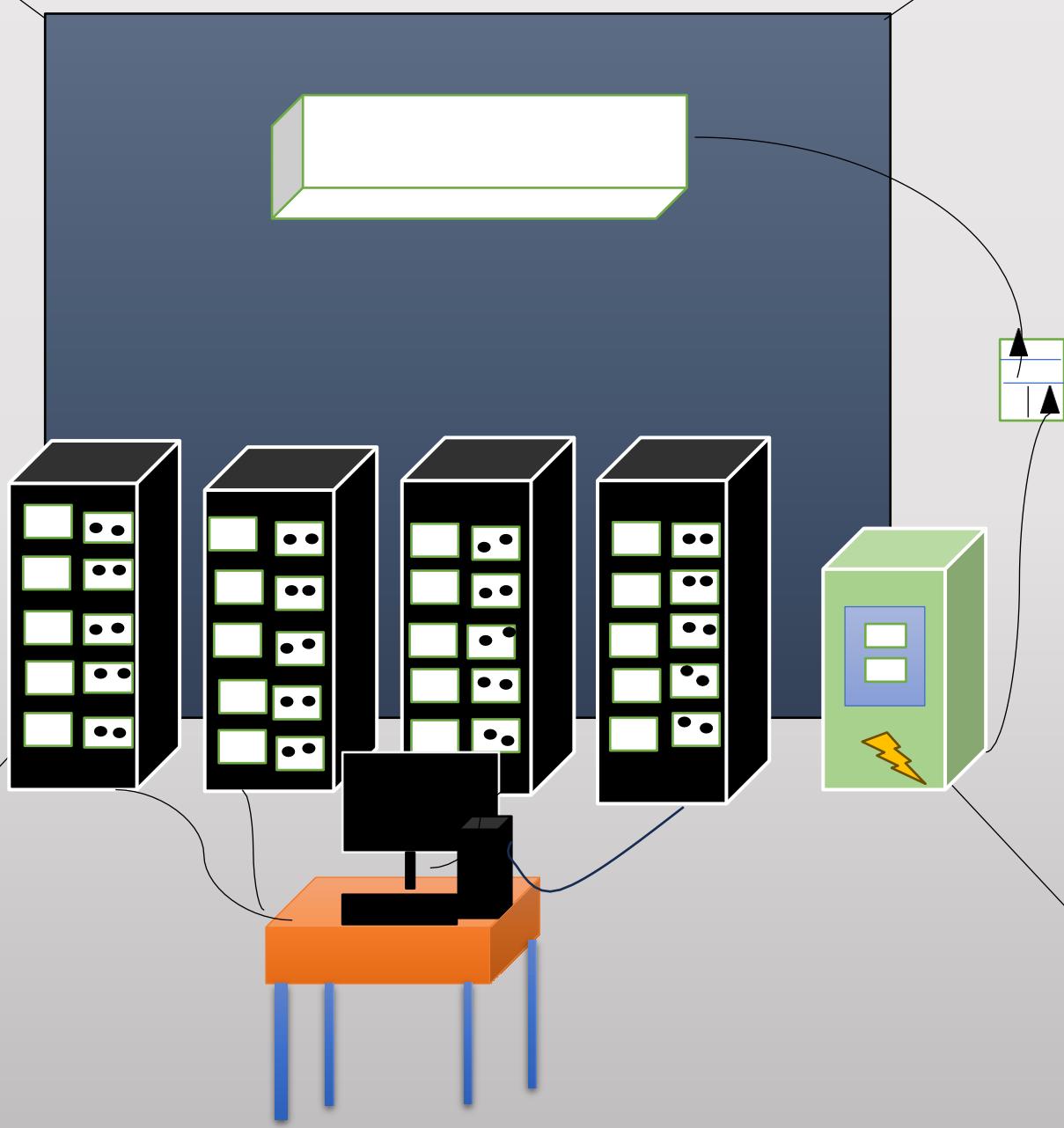
PROJECT 2:

Design a computer lab Connecting switches and routers.



PROJECT 3

Design a computer lab with server block



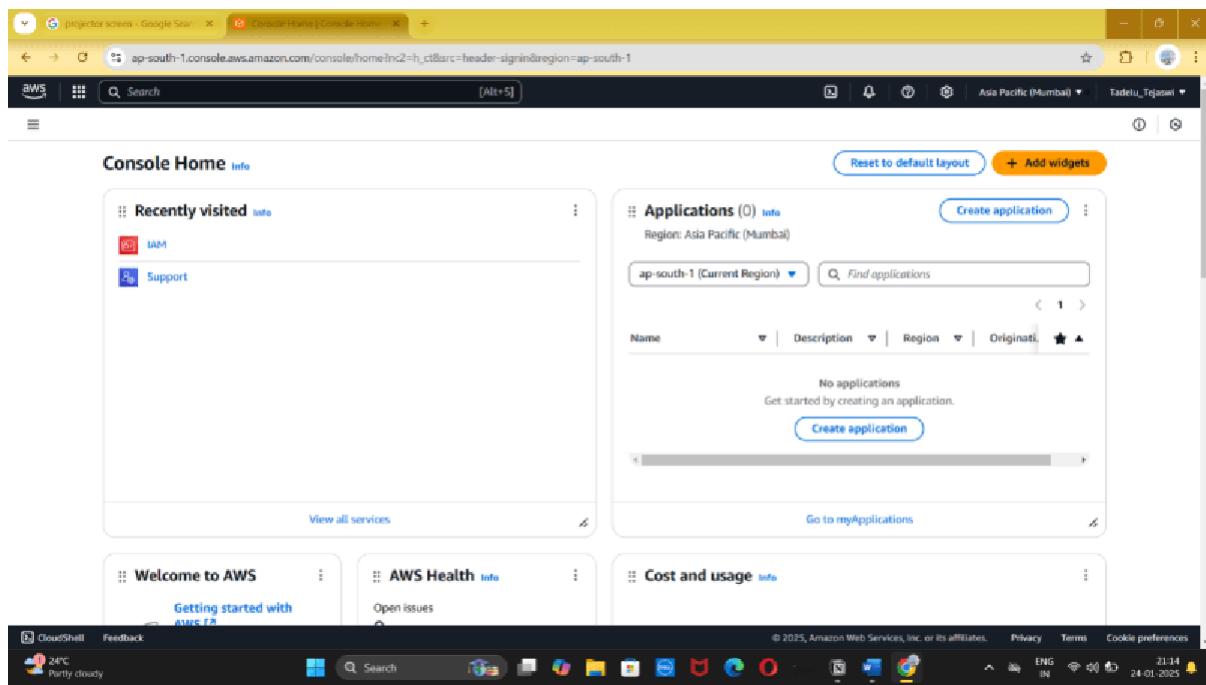
PROJECT 4

Cloud console services

Step 1: Sign in to management console home page.



Step 2: The console home page will be loaded.



Step 3: Now select Mumbai region

The screenshot shows the AWS Console Home page. On the right side, there is a sidebar titled "Region" which lists various AWS regions. The "Asia Pacific (Mumbai)" region is selected, as indicated by the blue background and the text "ap-south-1 (Current Region)". Other regions listed include United States (N. Virginia, Ohio, N. California, Oregon), Asia Pacific (Mumbai) (Mumbai, Osaka, Seoul, Singapore, Sydney, Tokyo), Canada (Central), Europe (Frankfurt, Ireland, London, Paris, Stockholm), and South America (São Paulo). The main content area shows sections for "Applications (0)", "Cost and usage", and "AWS Health".

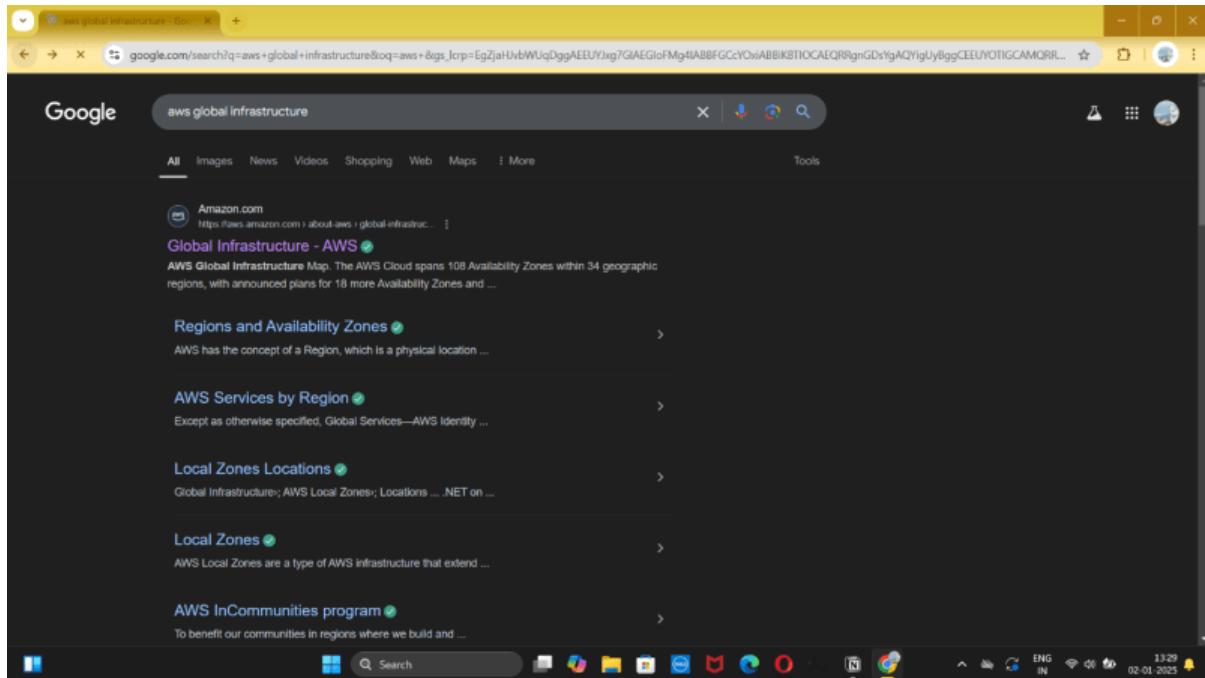
Step 4: Show the services available

The screenshot shows the AWS Console Home page with the service navigation sidebar expanded on the left. The sidebar includes sections for "Recently visited" (Console Home, IAM, Support), "Analytics", "Application Integration", "Blockchain", "Business Applications", "Cloud Financial Management", "Compute", "Containers", "Customer Enablement", "Database", "Developer Tools", "End User Computing", "Front-end Web & Mobile", "Game Development", "Internet of Things", "Machine Learning", "Management & Governance", and "Media Services". The main content area shows sections for "Applications (0)", "Cost and usage", and "AWS Health".

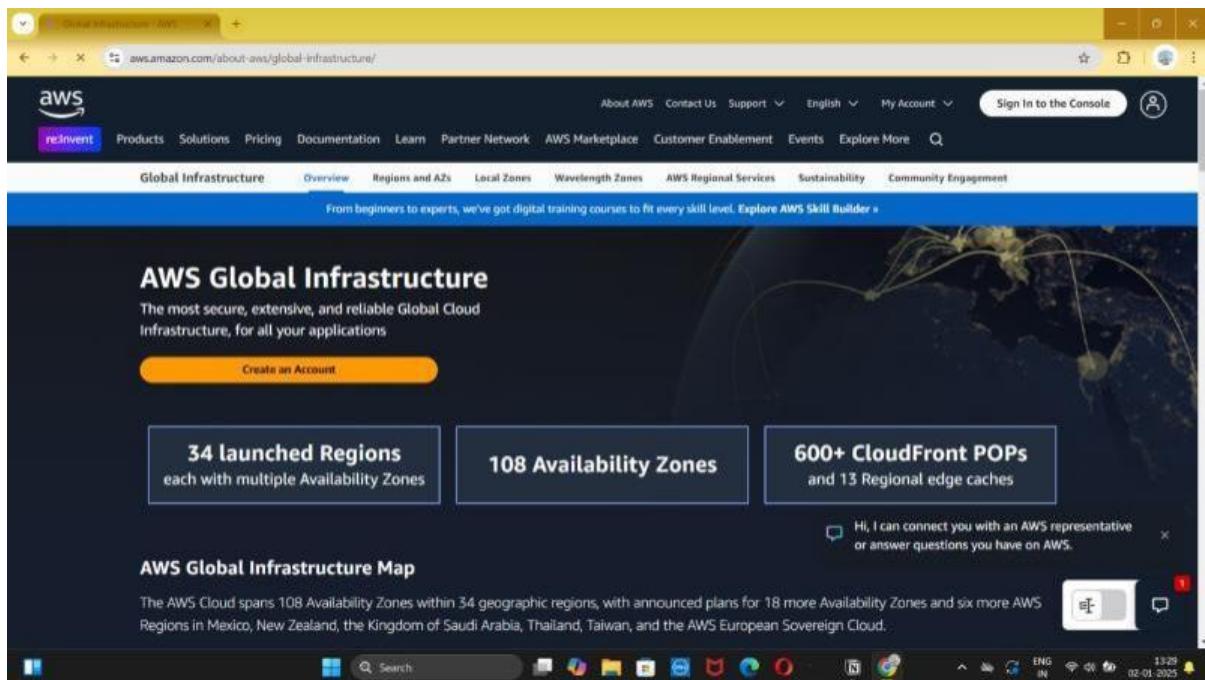
PROJECT 5

AWS GLOBAL INFRASTRUCTURE

Step 1: Search AWS Global Infrastructure.



Step 2: Now click on AWS Regional services



Step 3: Now show the list of services available.

The screenshot shows the AWS Services by Region page. The URL is aws.amazon.com/about-aws/global-infrastructure/regional-product-services/?p=ngi&loc=4&refid=09863622-0e2a-4080-9bba-12d378a294ba. The page title is "List of AWS Services Available by Region". A sidebar on the left lists "List of AWS Services Available by Region", "AWS Edge Network Locations", "AWS China Regions*", and "AWS Support in AWS GovCloud (US)". The main content area shows a dropdown menu for "Region" set to "US East (N. Virginia)". Below it, a list of "Services Offered" includes AWS Amplify, AWS App Mesh, AWS App Runner, AWS AppFabric, AWS AppSync, AWS Application Discovery Service, AWS Application Migration Service (MGN), AWS Artifact, and AWS Audit Manager. A tooltip message "Hi, I can connect you with an AWS representative or answer questions you have on AWS." is visible. The bottom of the screen shows a Windows taskbar with various icons and the date/time "02-01-2025".

Step 4: Now click on the list of servies

The screenshot shows the same AWS Services by Region page as before, but the "Region" dropdown menu is now expanded, showing a list of regions and availability zones. The expanded list includes:

- US East (N. Virginia) - us-east-1
- US East (Ohio)
- US West (N. California)
- US West (Oregon)
- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- Asia Pacific (Hyderabad)
- Asia Pacific (Jakarta)
- Asia Pacific (Malaysia)
- Asia Pacific (Melbourne)
- Asia Pacific (Mumbai)
- Asia Pacific (Osaka)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- ap-southeast-1
- ap-southeast-2
- ap-southeast-3
- ap-southeast-4
- ap-southeast-5

The rest of the page content remains the same, including the sidebar, service list, and tooltip message. The Windows taskbar at the bottom is also present.

Step 5: Choose Mumbai region.

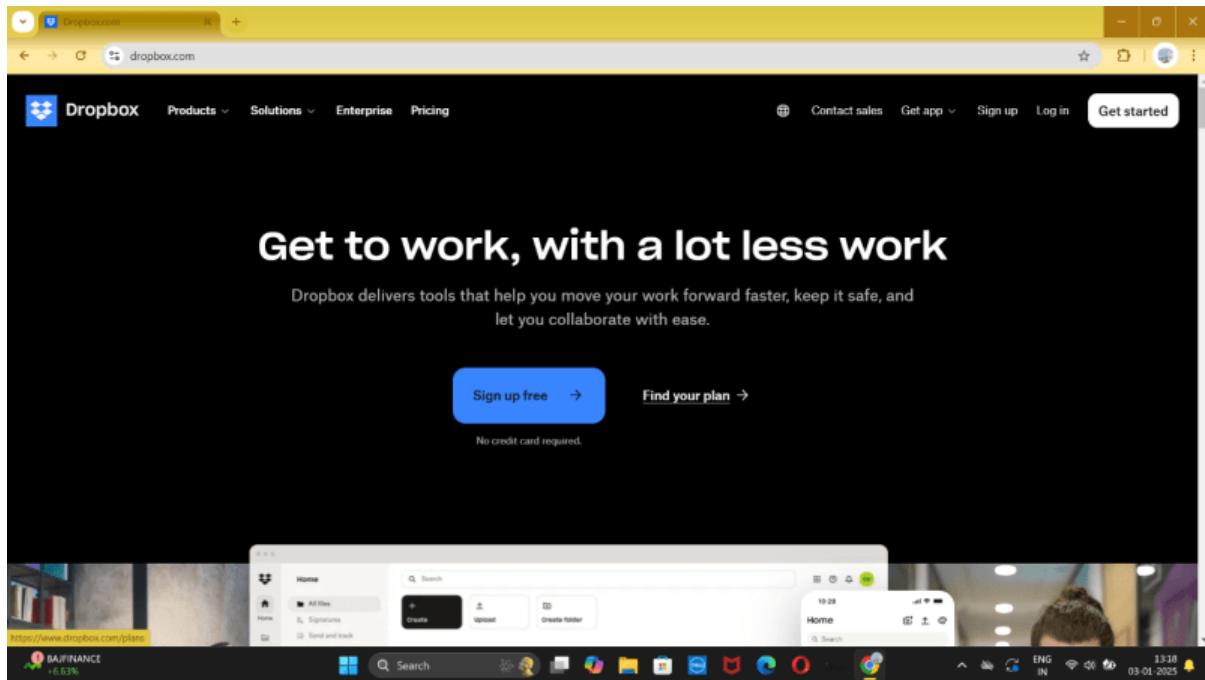
The screenshot shows a web browser displaying the AWS Global Infrastructure page. The URL in the address bar is aws.amazon.com/about-aws/global-infrastructure/regional-product-services/?p=ngi&loc=4&refid=09863622-0e2a-4080-9bba-12d378a294ba. The page title is "AWS Services by Region - AWS". The navigation bar includes links for "About AWS", "Contact Us", "Support", "English", "My Account", and "Sign In to the Console". The main menu has categories like "Products", "Solutions", "Pricing", "Documentation", "Learn", "Partner Network", "AWS Marketplace", "Customer Enablement", "Events", "Explore More", and a search bar. A sub-menu for "Regions and AZs" is open, showing "Region" dropdown set to "Asia Pacific (Mumbai)". The "AWS Regional Services" section lists various services offered in the Mumbai region, including AWS Amplify, AWS App Mesh, AWS App Runner, AWS AppSync, AWS Application Migration Service (MGN), AWS Artifact, AWS Audit Manager, AWS Auto Scaling, AWS Backup, AWS Batch, AWS Budgets, and AWS Certificate Manager. A tooltip message from an AI representative is visible, stating "Hi, I can connect you with an AWS representative or answer questions you have on AWS." The system tray at the bottom right shows the date as 02-01-2025 and time as 13:29.

PROJECT 6

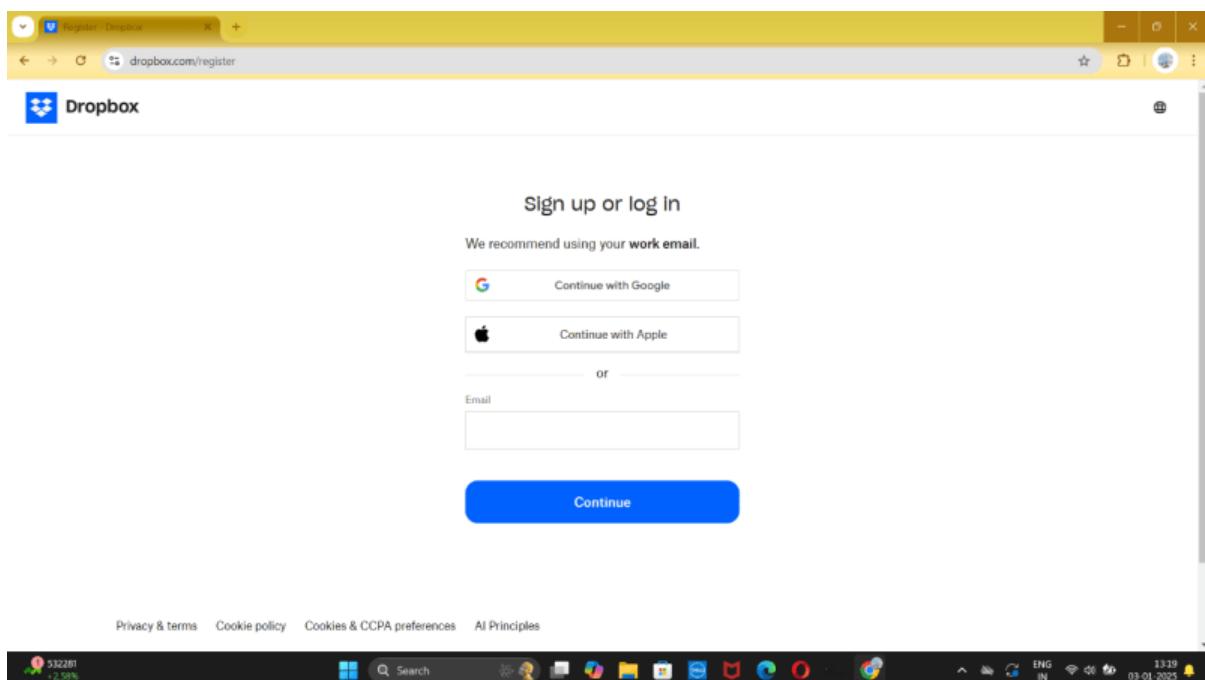
DROP BOX.COM

CREATE A FILE STORAGE IN DROPBOX

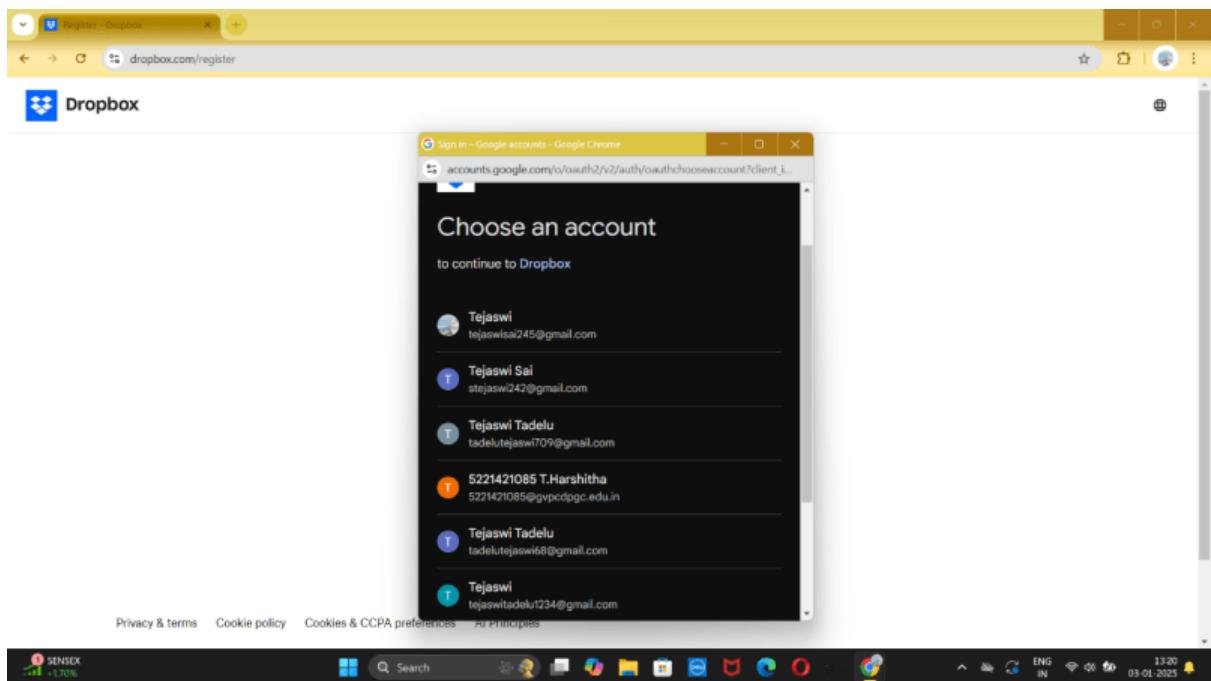
Step 1: Go to Google and type dropbox.com to open official drop box website



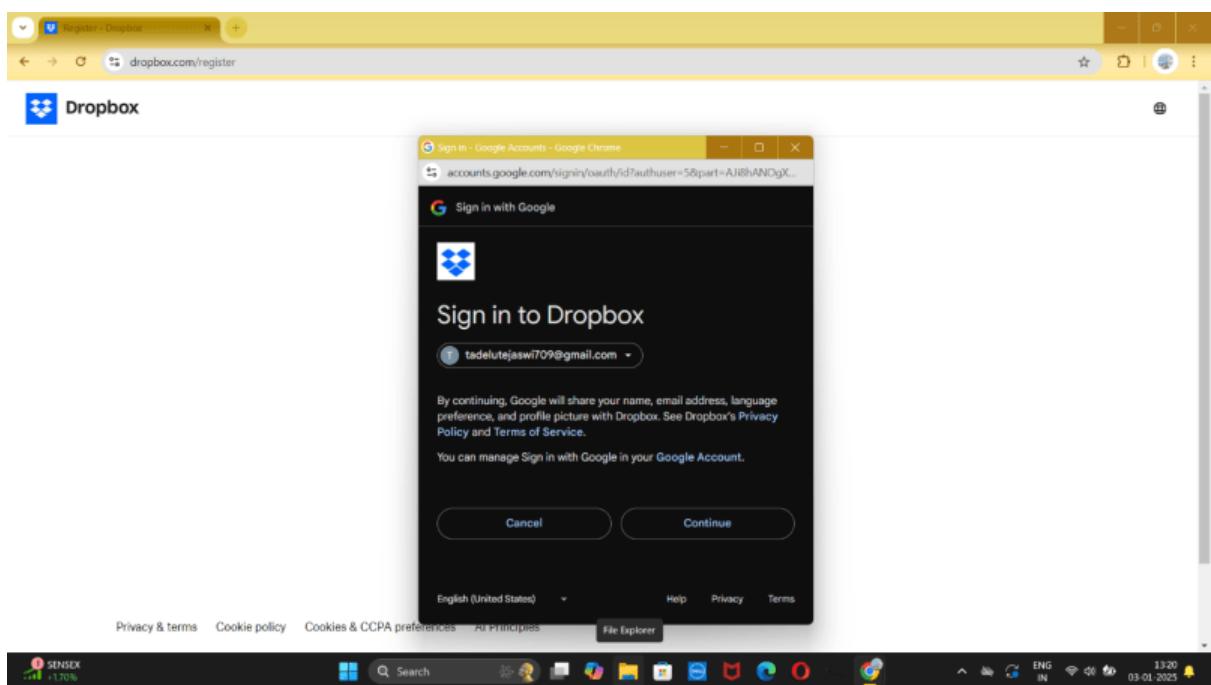
Step 2: Sign up or login page occurs to login or signup to portal



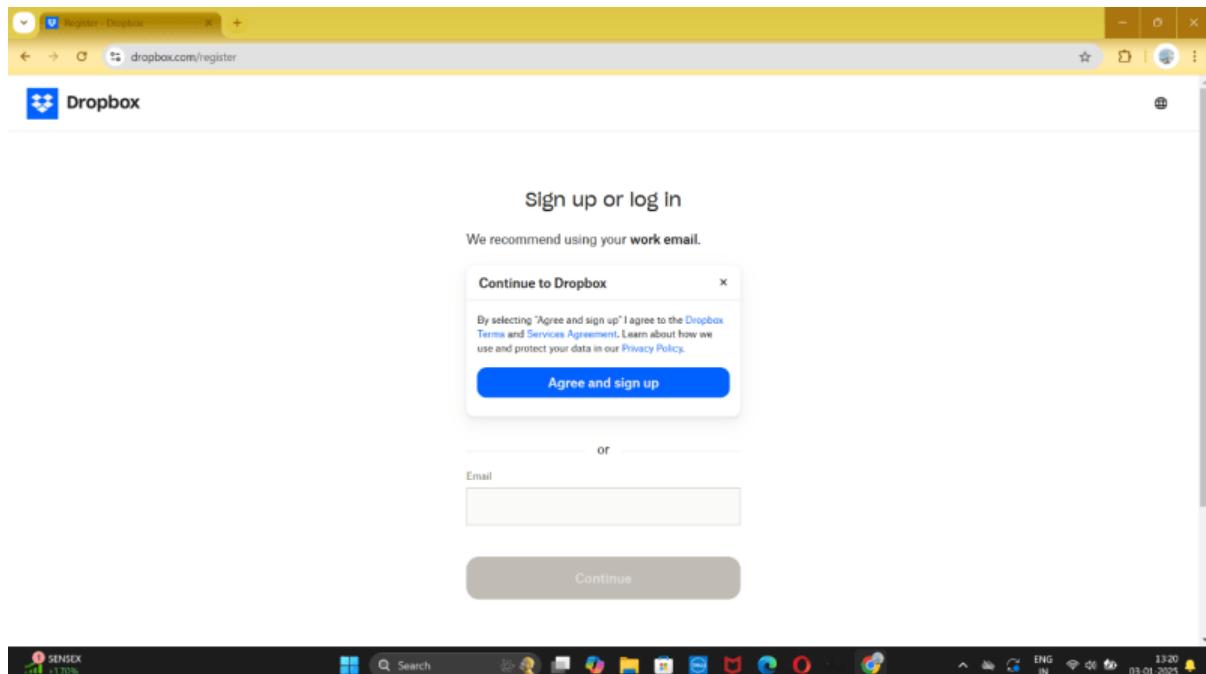
Step 3: Now click on choose an account or type mail id and password



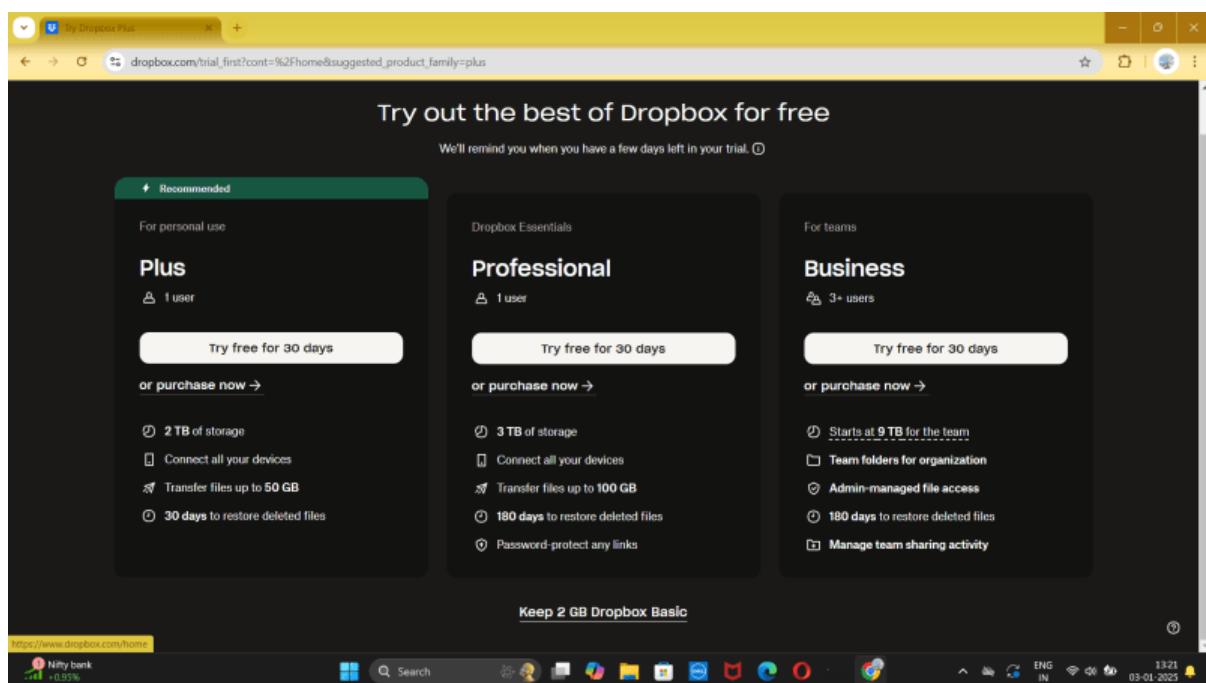
Step 4: Click on sign in to drop box and continue



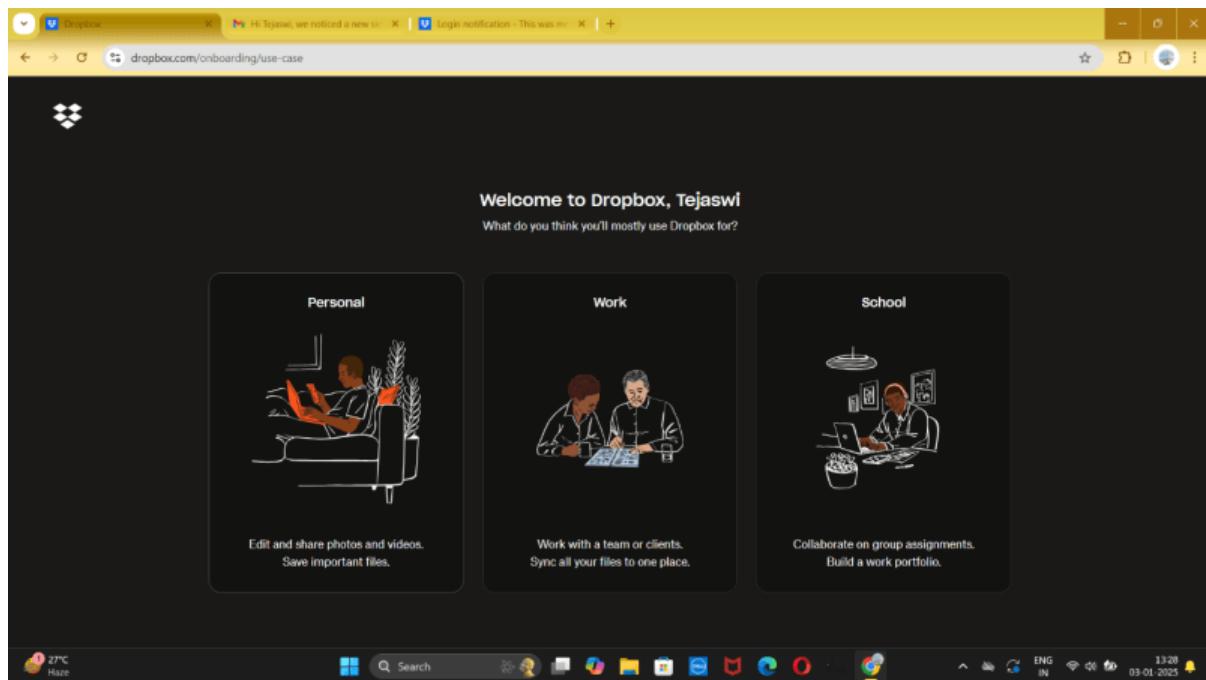
Step 5: Now click on agree and continue and then continue to open dropbox official portal



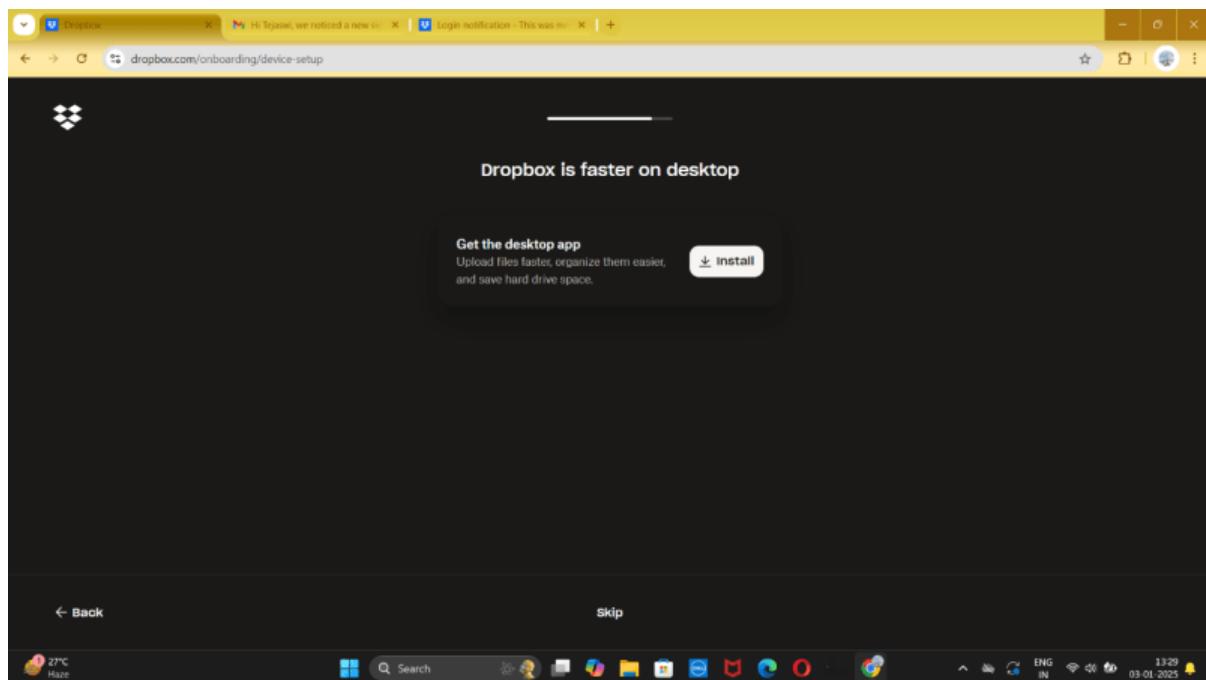
Step 6: In the following plans click on basic 2GB plan for free access of drop box.



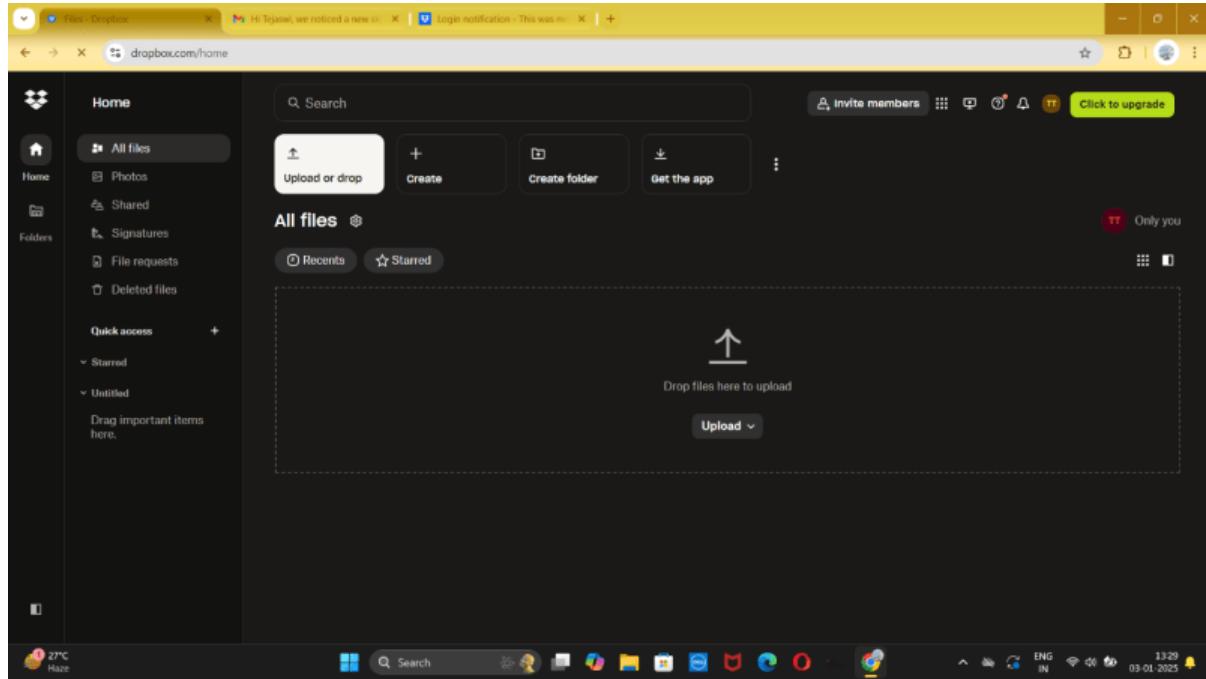
Step 7: Welcome to drop box appears appears and click on Personal.



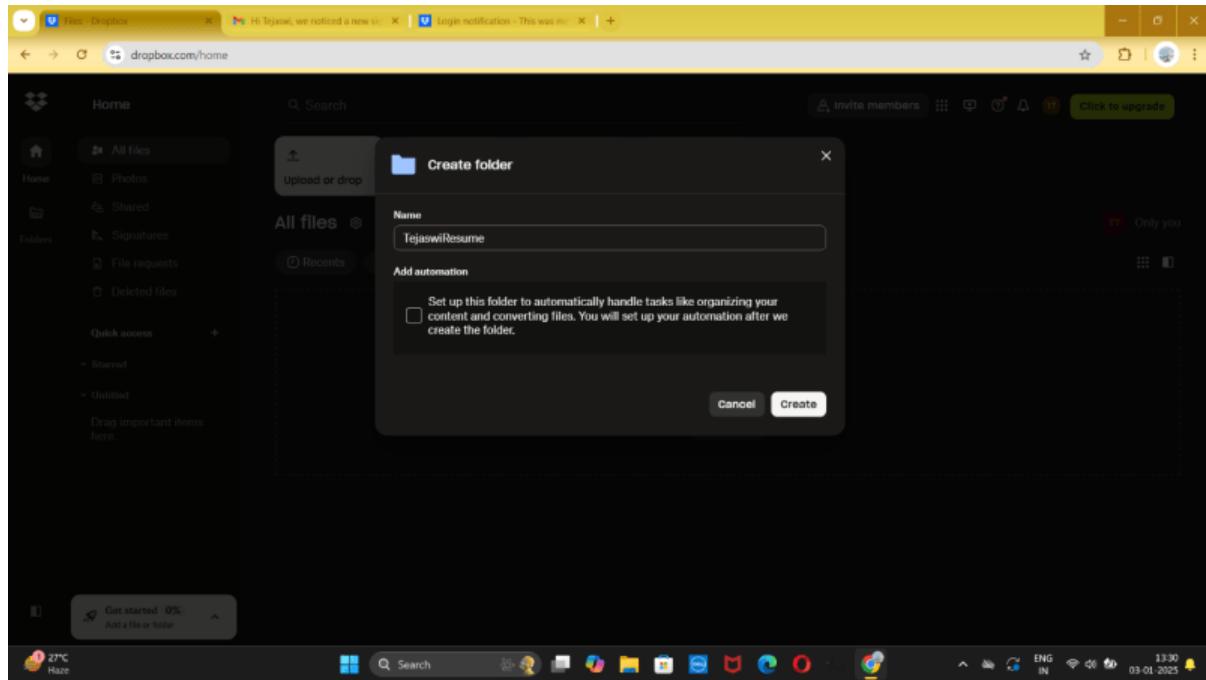
Step 8: Get the desktop site appears, if necessary, click on install in order to add as desktop icon of Dropbox.



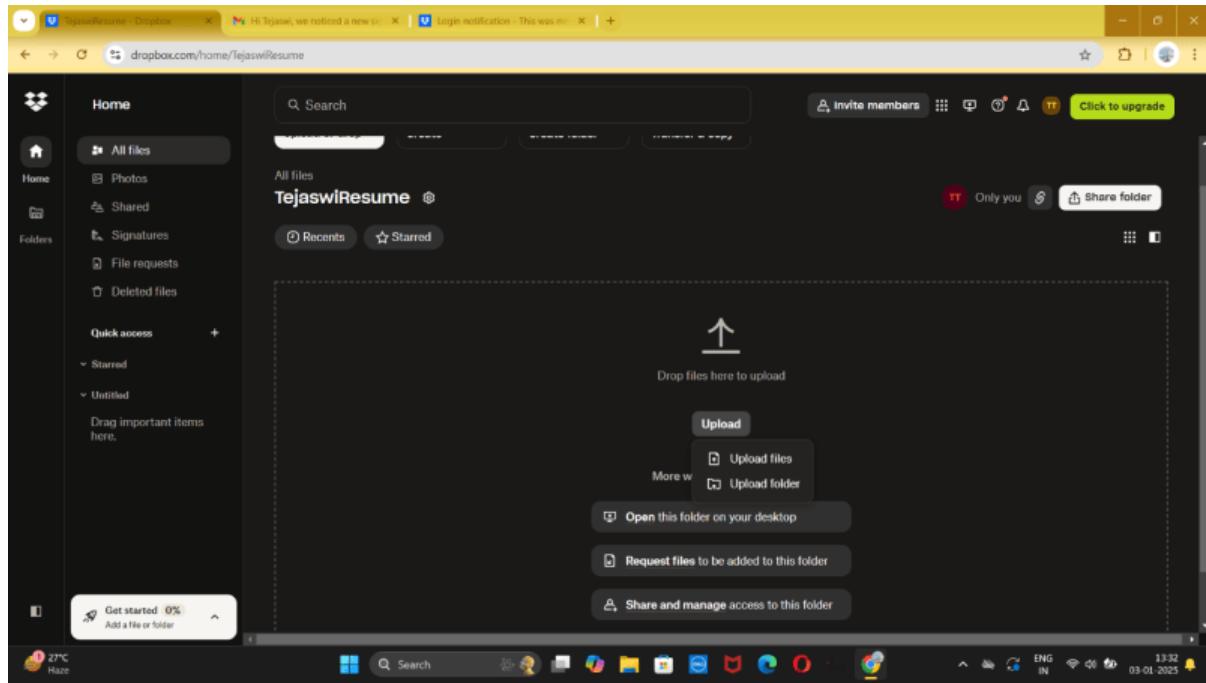
Step 9: The official portal of Dropbox appears and click on new folder.



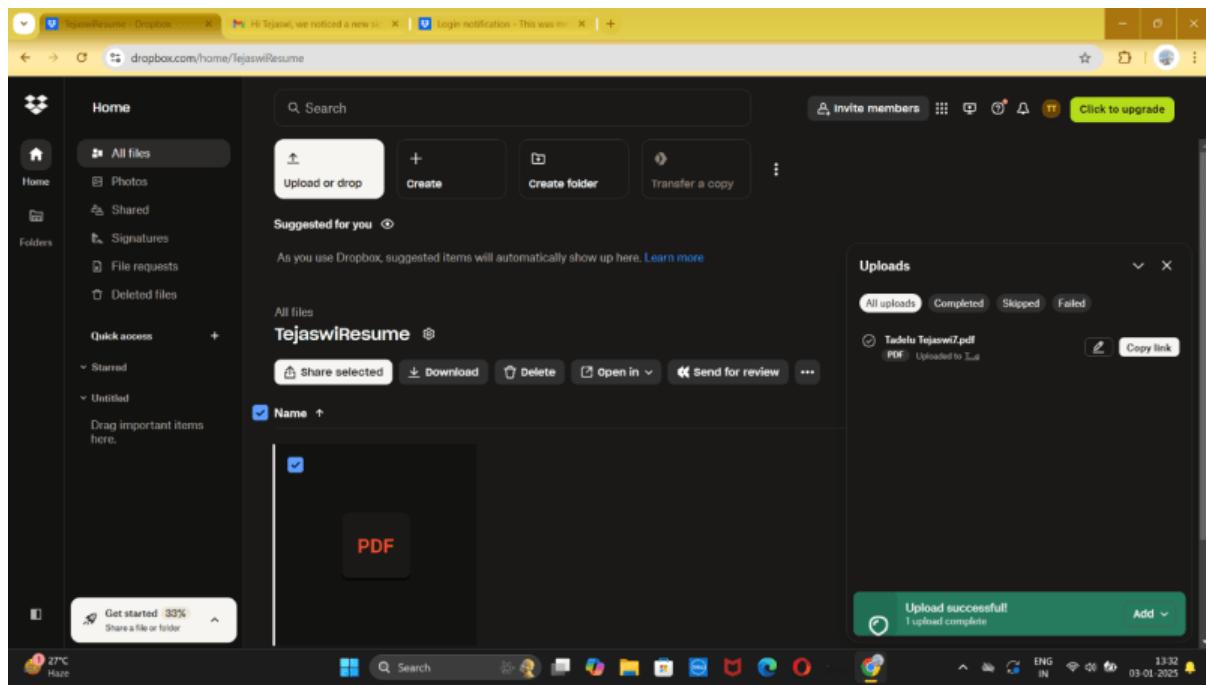
Step 10: Name the folder and click on create.



Step 11: The new folder appears and click on upload to upload resume.



Step 12: The resume is uploaded successfully as a new file in the created folder.

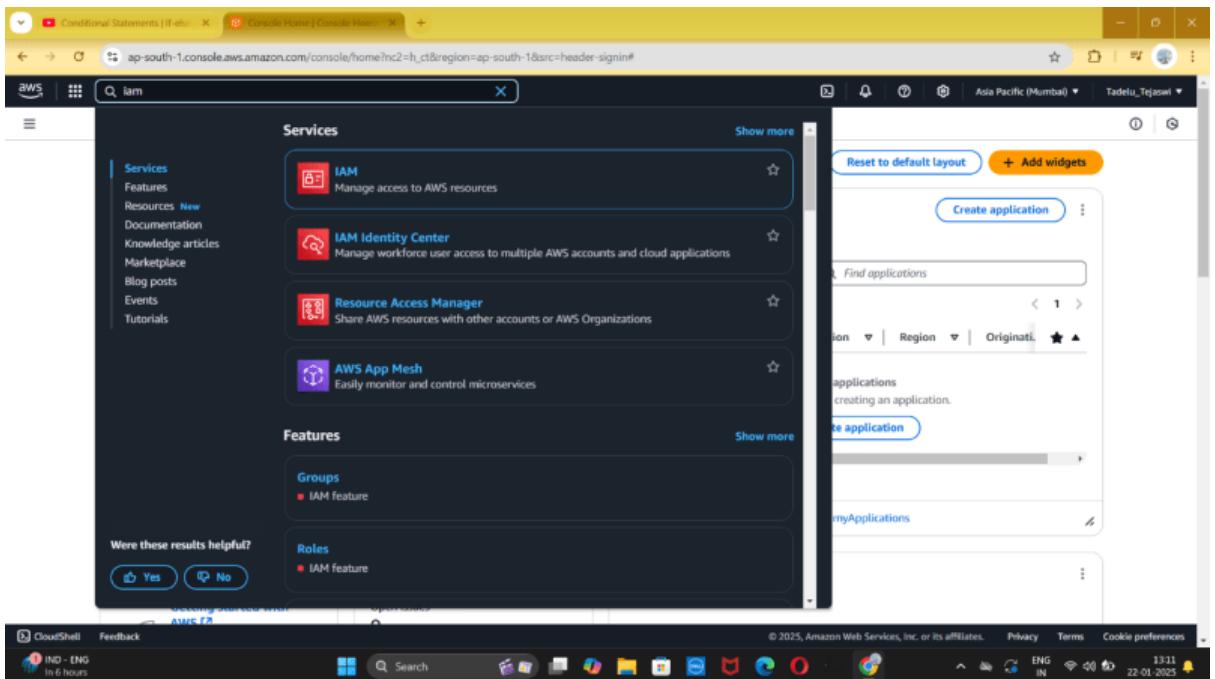


Step 13: The resume is uploaded successfully as a new file in the created folder.

PROJECT 7

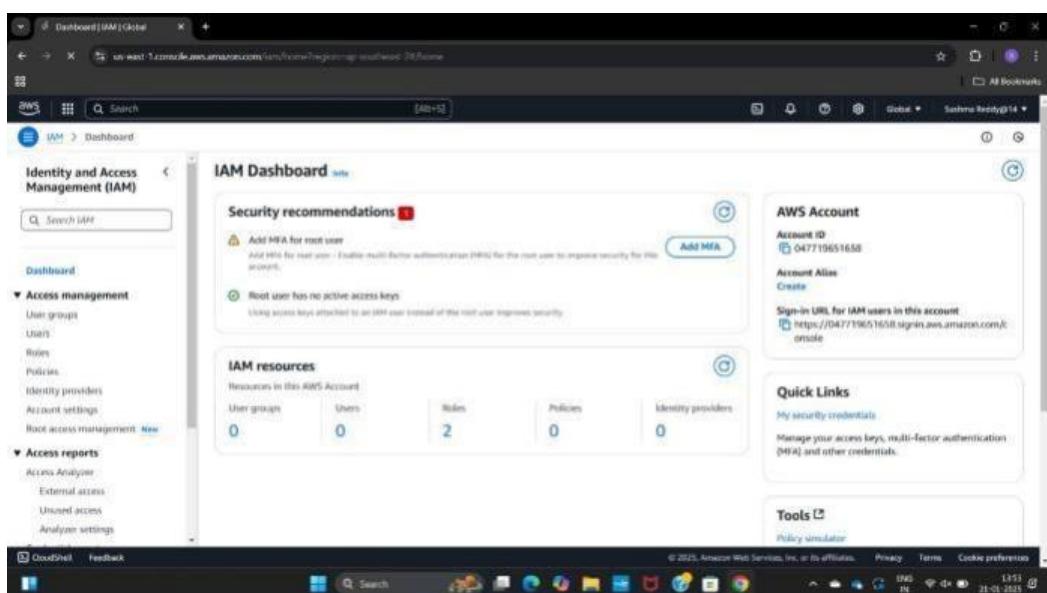
Step 1:-Create an IAM(Identify Access Management) user account

- Sign into the AWS Management Console



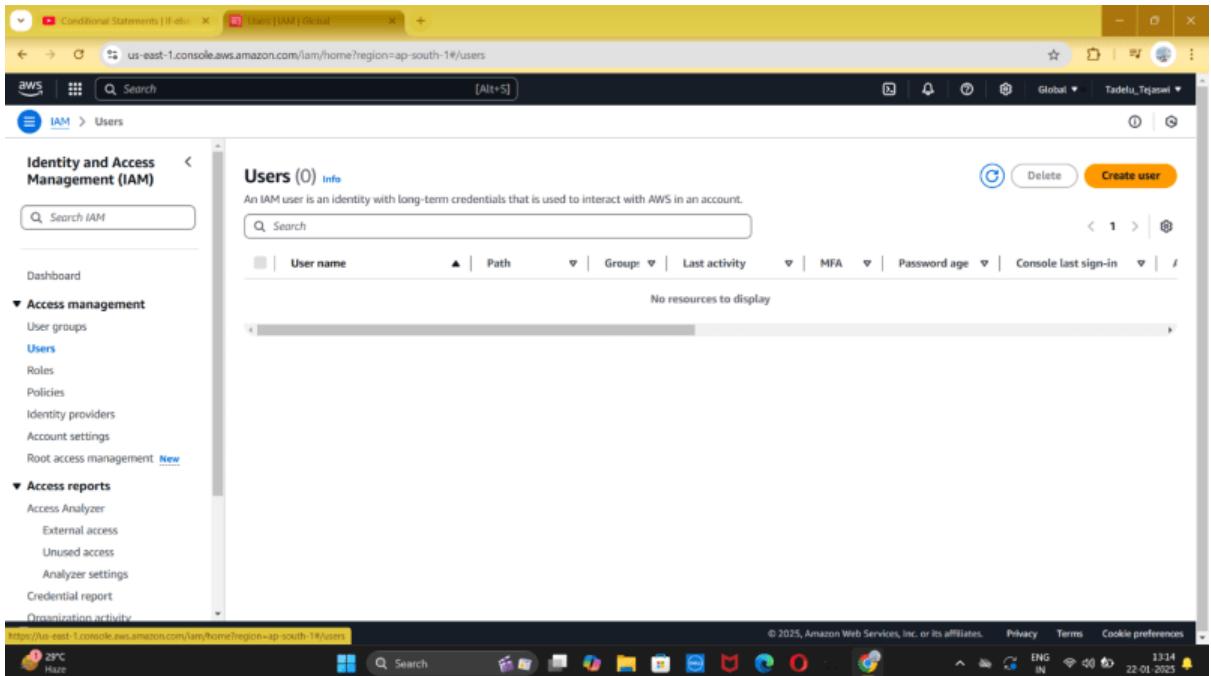
Step 2:- Security recommendations

- Choose the option “users groups” in the access management



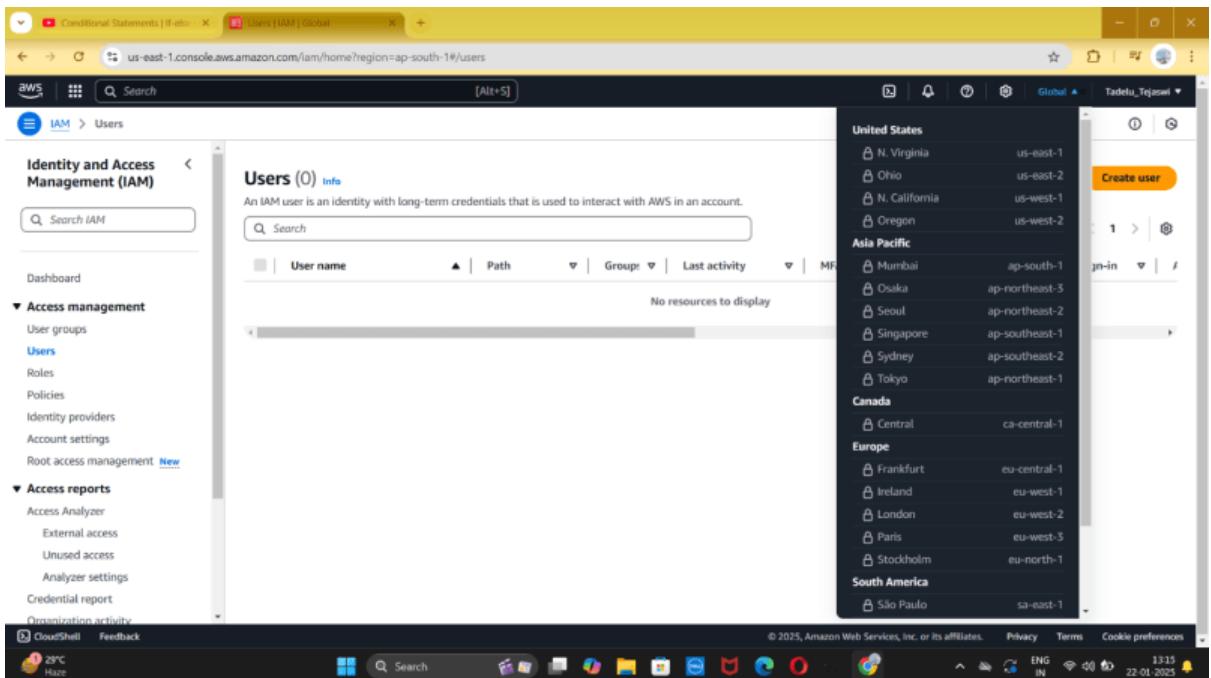
Step 3:- Users

- Select create user



Step 4:-Service global

- IAM is a web service that lets you control access to AWS resources



Step 5:- Create users

- Now create the username and click the next option

Screenshot of the AWS IAM 'Create user' wizard Step 1: Specify user details.

The user name is set to 'Tejaswi@23'. A note states: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + @ _ - (hyphen)'.

Provide user access to the AWS Management Console - optional

If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

Important: If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Buttons: Cancel, Next



Screenshot of the AWS IAM 'Create user' wizard Step 1: Specify user details.

The user name is set to 'Tejaswi@23'. A note states: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + @ _ - (hyphen)'.

Provide user access to the AWS Management Console - optional

If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

Are you providing console access to a person?

Specify a user in Identity Center - Recommended

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Important: If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Buttons: Cancel, Next

Step 7:- Create custom password

Conditional Statements [If-else] Create user | IAM | Global

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#users/create

IAM > Users > Create user

Are you providing console access to a person?

User type

Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

Autogenerated password
You can view the password after you create the user.

Custom password
Enter a custom password for the user.
Vyasan@123

Show password

Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 29°C Haze ENG IN 13:17 22-01-2025

Screenshot of the AWS IAM 'Create user' wizard - Step 2: Set permissions.

The page title is 'Create user (IAM | Global)'. The left sidebar shows steps: Step 1 (Specify user details), Step 2 (Set permissions, currently selected), Step 3 (Review and create), and Step 4 (Retrieve password).

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

- Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
- Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

[Create group](#)

Get started with groups
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

Set permissions boundary - optional

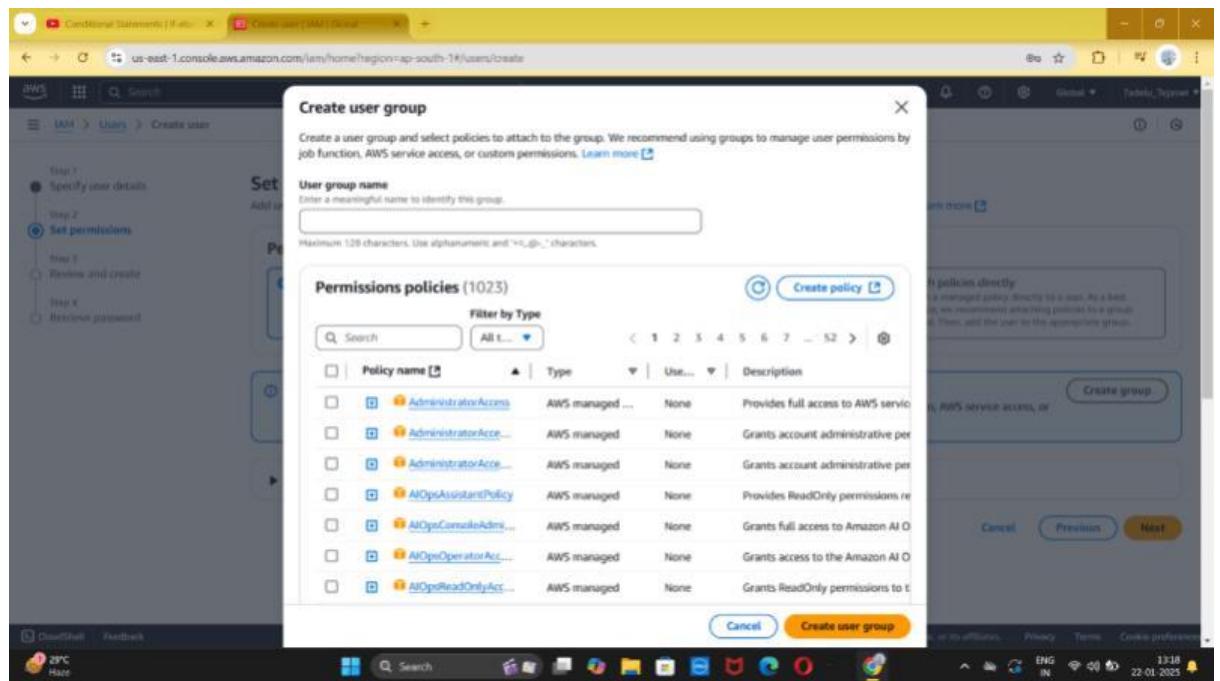
Cancel Previous Next



Project-8

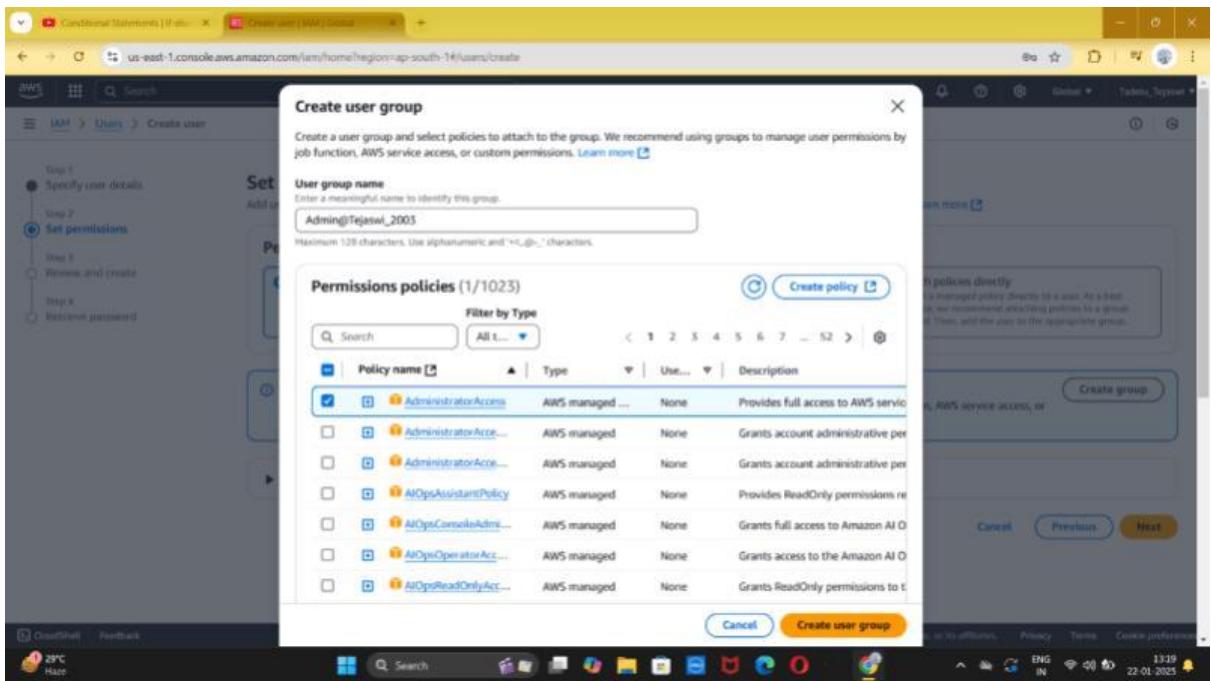
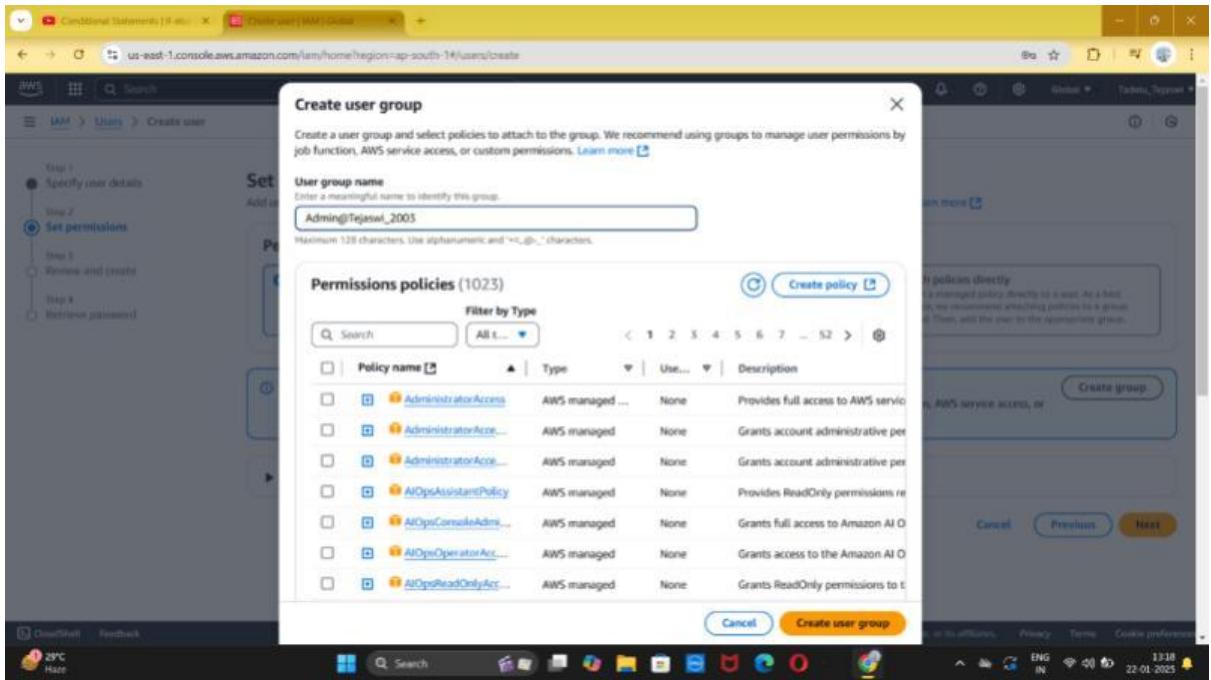
- Create a group in IAM

Step 1:- Click on create group



Step 2:-Create group

- Give the username before creating the group



Step 3:-Choose policy name and click on create user group

Permissions options

- Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
- Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (1/1)			
<input type="text"/> Search			
Group name	Users	Attached policies	Created
<input checked="" type="checkbox"/> Admin@Tejaswi_2003	0	AdministratorAccess	2025-01-22 (2 minutes ago)

▶ Set permissions boundary - optional

Cancel Previous Next

Step 4:
Add user into admin group and click on next.

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details	Console password type	Require password reset
User name Tejaswi@23	Custom password	Yes

Name	Type	Used as
Admin@Tejaswi_2003	Group	Permissions group
IAMUserChangePassword	AWS managed	Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 13:20 22-01-2025

Conditional Statements | If-else X Create user | IAM | Global X +

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create

aWS Search [Alt+S]

IAM > Users > Create user

Admin@Tejaswi_2003 user group created.

Review and create Step 4 Retrieve password

User name Tejaswi@23 Console password type Custom password Require password reset Yes

Permissions summary

Name	Type	Used as
Admin@Tejaswi_2003	Group	Permissions group
IAMUserChangePassword	AWS managed	Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

Key Value - optional

Computer applications BCA-B Remove

Add new tag You can add up to 49 more tags.

Create user Previous Cancel

CloudShell Feedback 29°C Haze Search Privacy Terms Cookie preferences © 2025, Amazon Web Services, Inc. or its affiliates. ENG IN 13:21 22-01-2025

Conditional Statements | If-else X Create user | IAM | Global X +

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create

aWS Search [Alt+S]

IAM > Users > Create user

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

View user

Step 1 Specify user details Step 2 Set permissions Step 3 Review and create Step 4 Retrieve password

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Console sign-in URL <http://841162666128.signin.aws.amazon.com/console> Email sign-in instructions

User name Tejaswi@23

Console password ***** Show

Cancel Download .csv file Return to users list

CloudShell Feedback 29°C Haze Search Privacy Terms Cookie preferences © 2025, Amazon Web Services, Inc. or its affiliates. ENG IN 13:22 22-01-2025

Conditional Statements | If else ... X Create user | IAM | Global X +

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create

IAM > Users > Create user

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Recent download history

- Tejaswi@23_credentials.csv 117 B - Done
- Head_First.Java.Second.Edition.pdf 45.2 MB + 1 hour ago

Full download history

Step 1 Specify user details
Step 2 Set permissions
Step 3 Review and create
Step 4 Retrieve password

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Console sign-in URL <https://841162666128.signin.aws.amazon.com/console>

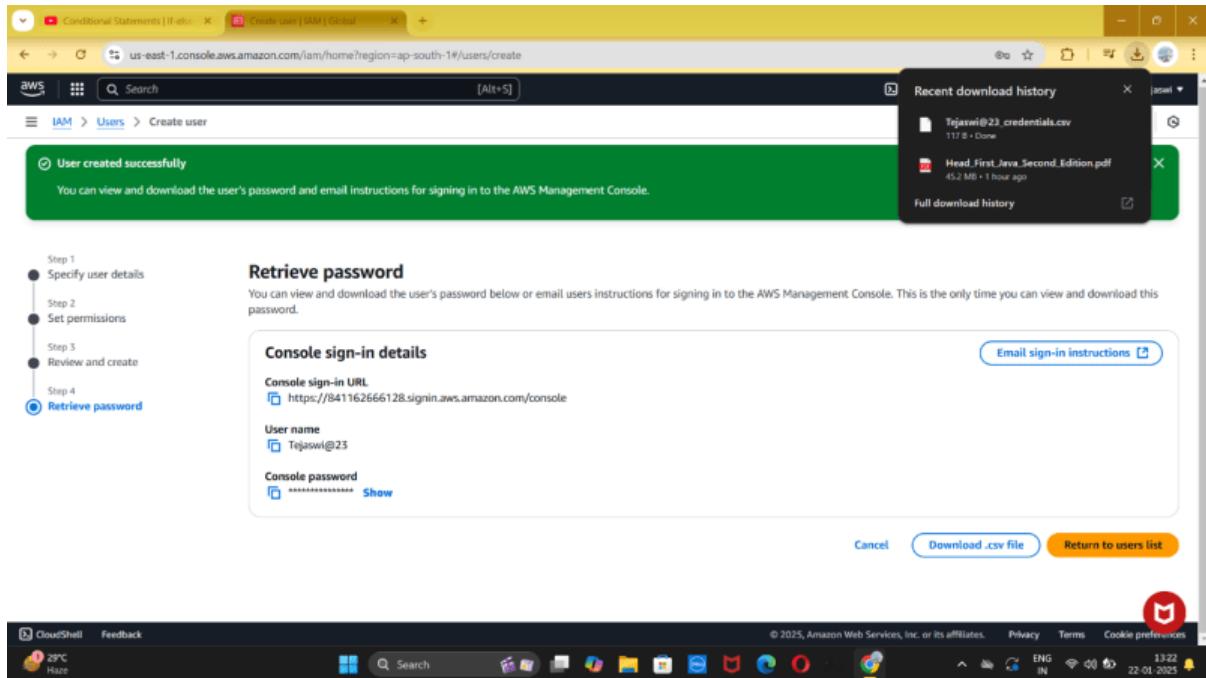
User name [Tejaswi@23](#)

Console password [*****](#) [Show](#)

Email sign-in instructions

Cancel Download .csv file Return to users list

CloudShell Feedback 29°C Rainy © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 13:22 22-01-2023



PROJECT 9

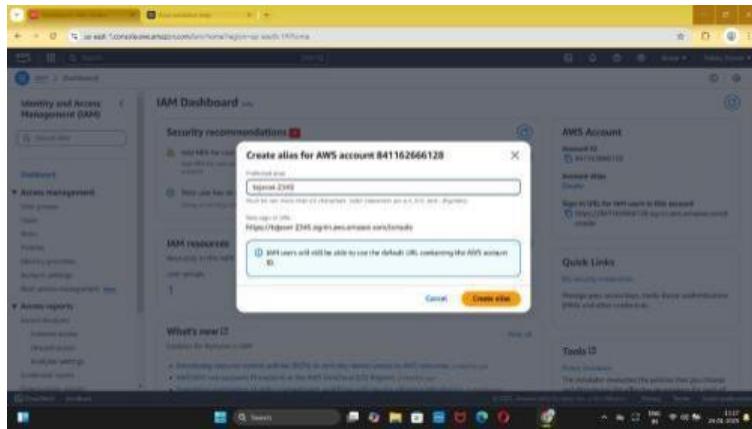
CREATE ALIAS ACCOUNT FOR YOUR AWS ACCOUNT

Step 1: Open AWS IAM dashboard

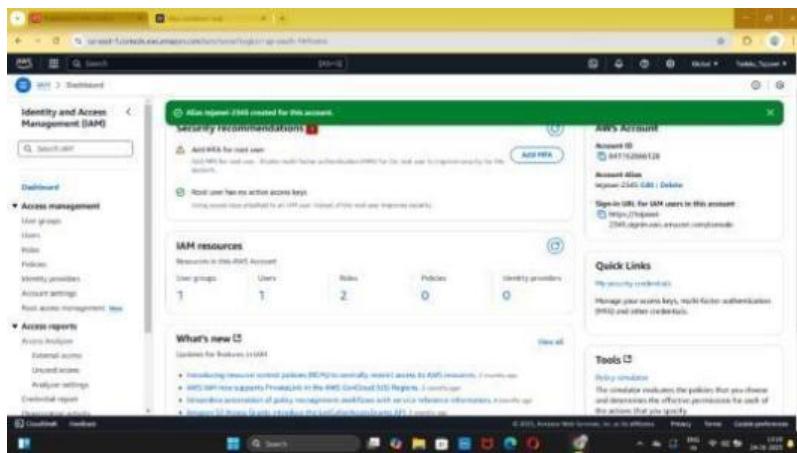
The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with navigation links like 'Identity and Access Management (IAM)', 'Access management', 'Access reports', and 'Access analyzer'. The main area has sections for 'Security recommendations' (with items like 'Add MFA for root user' and 'Root user has no active access keys'), 'IAM resources' (showing 1 User group, 1 User, 2 Roles, 0 Policies, 0 Identity providers), and 'What's new' (listing recent updates). To the right, there's a 'AWS Account' summary with the Account ID '841162666128' and an 'Account Alias' section with a 'Create' button. A 'Quick Links' box and a 'Tools' box are also present.

Step 2: Give the user id for creating the alias AWS account.

This screenshot is similar to the first one, showing the IAM Dashboard. However, a modal window titled 'Create alias for AWS account 841162666128' is open in the center. It contains a single input field labeled 'Preferred alias' with the placeholder 'aliasname' and a note below it. At the bottom of the modal are 'Cancel' and 'Create alias' buttons. The rest of the dashboard interface remains visible in the background.

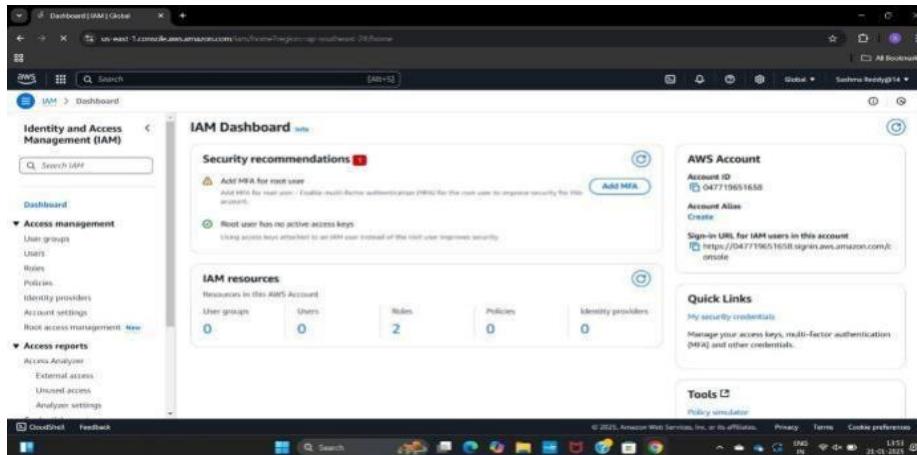


Step 3: Successfully user id will be created.

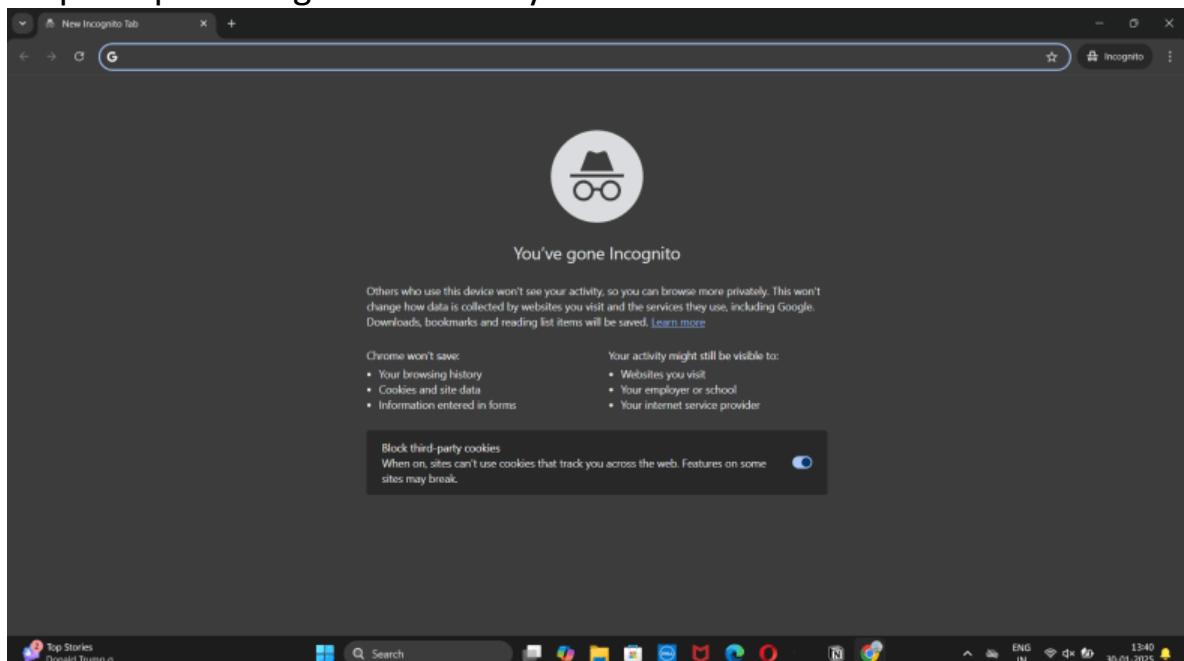


PROJECT – 10

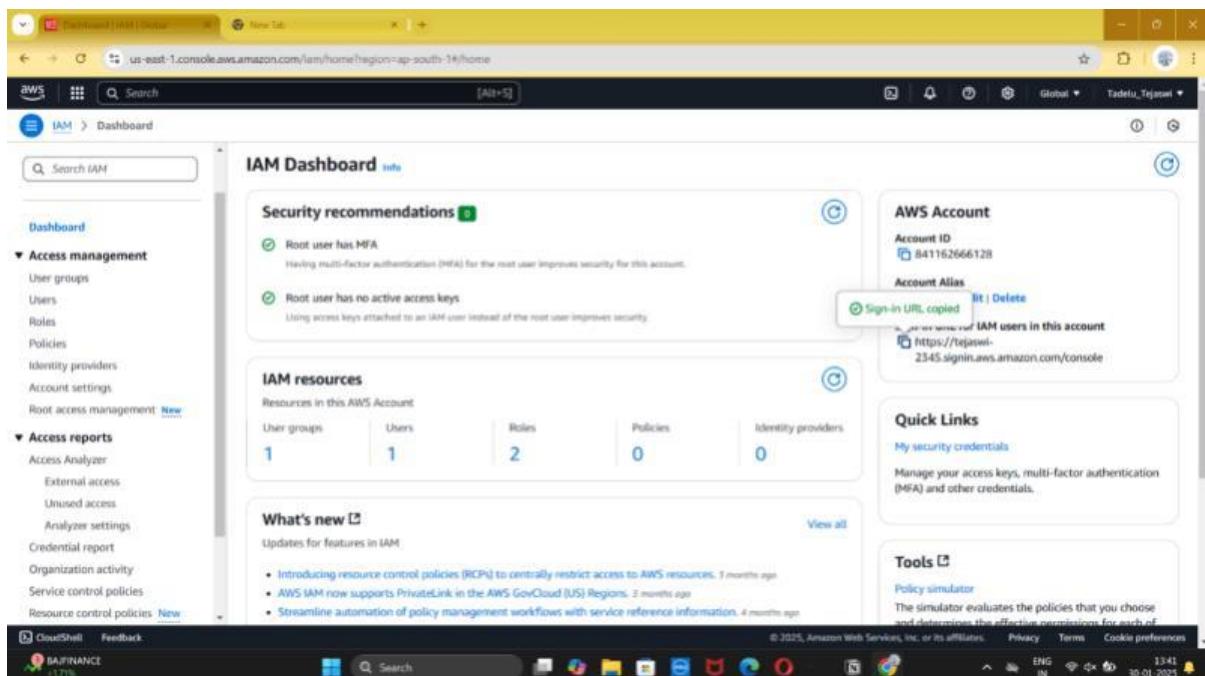
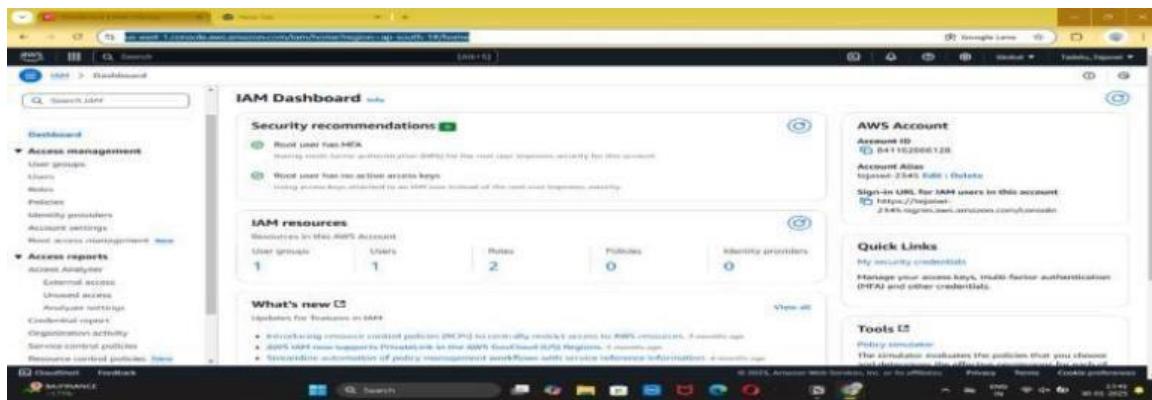
Step 1: Open AWS management console and select IAM Dashboard



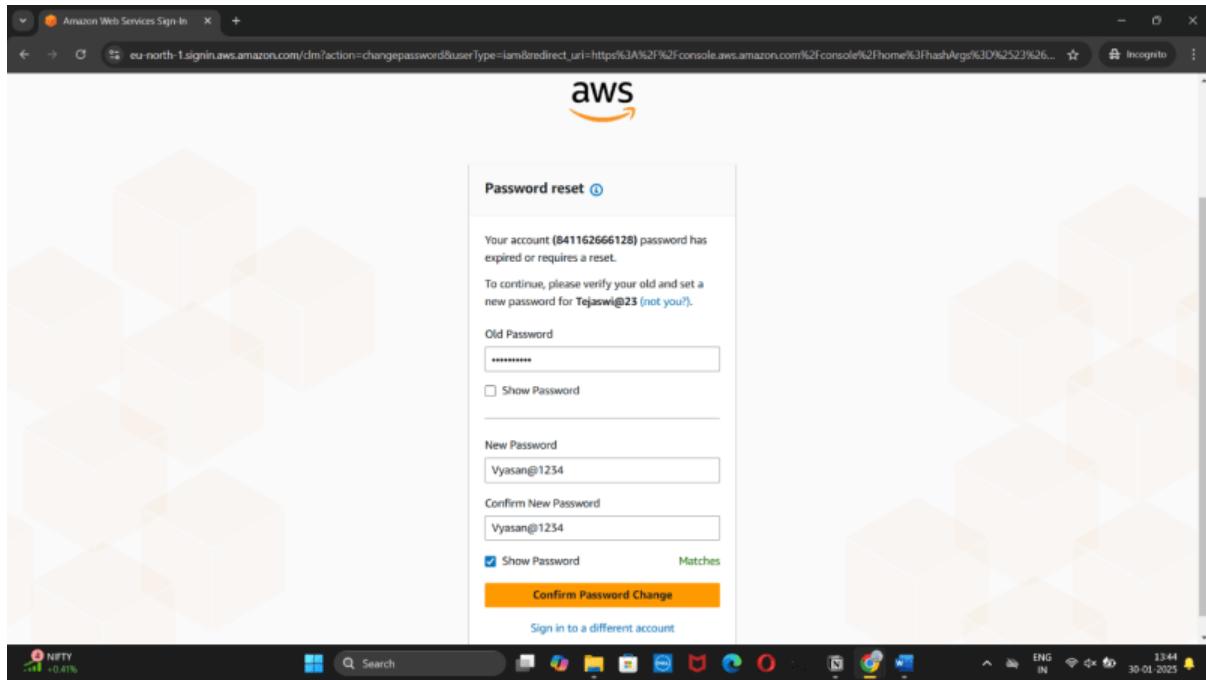
Step 2: Open Incognito tab in any web browser.



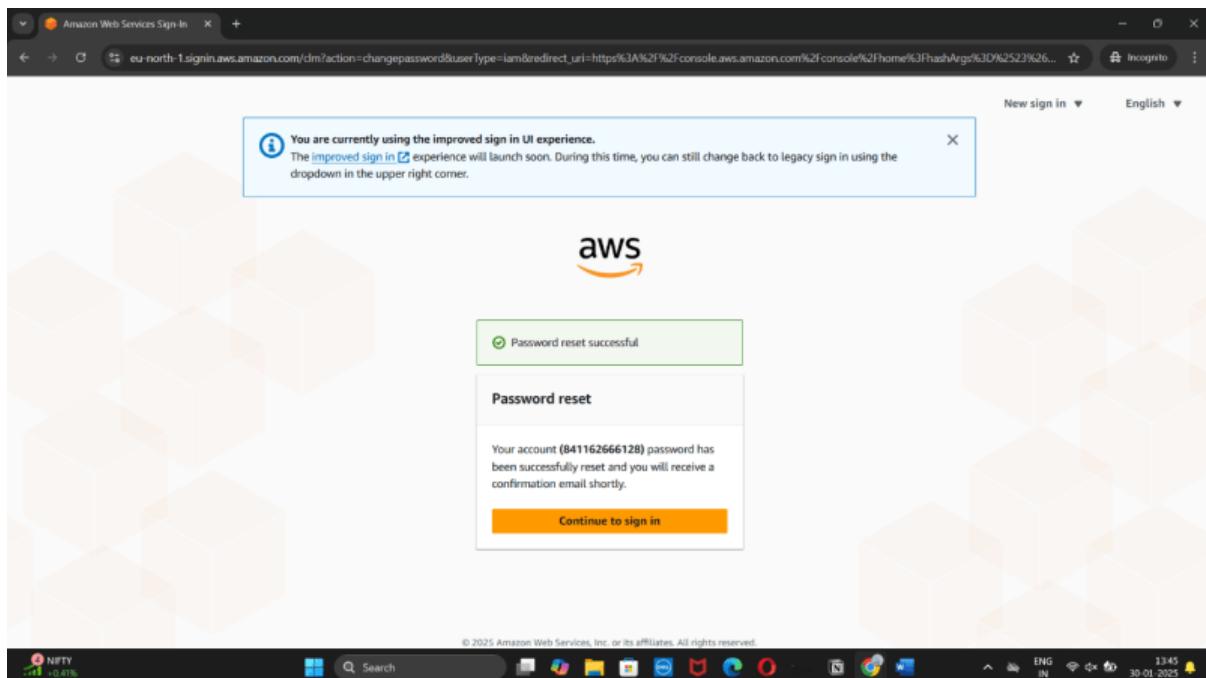
Step 3: Copy the URL and press it and enter.



Step 4: Set password and username as per IAM.



Step 5: Password set automatically.



Step 6: IAM Dashboards and accounts.

The image shows two identical screenshots of the AWS IAM Dashboard side-by-side, likely demonstrating a feature or a bug. Both screens are titled "IAM | Global" and show the "Dashboard" view for an account with Account ID 8411-6266-6128.

Left Dashboard View:

- Security records:**
 - Root user has MFA: Having multi-factor authentication for this account improves security.
 - Root user has no active access keys: Using access keys after 90 days improves security.
- IAM resources:** Resources in this AWS Account
 - User groups: 1
 - Users: 1
 - Roles: 2
 - Policies: 0
 - Identity providers: 0

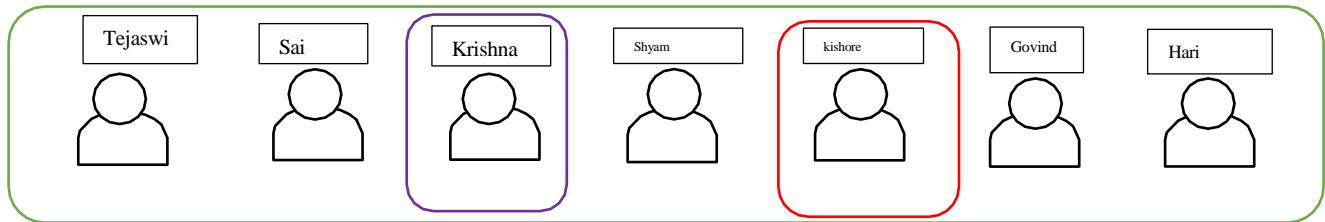
Right Dashboard View:

- Security records:**
 - Root user has MFA: Having multi-factor authentication for this account improves security.
 - Add MFA for yourself: Add multi-factor authentication for this account.
 - Your user, Tejaswi@23, does not have any active access keys that have been unused for more than a year. Deactivating or deleting unused access keys improves security.
- IAM resources:** Resources in this AWS Account
 - User groups: 1
 - Users: 1
 - Roles: 2
 - Policies: 0
 - Identity providers: 0

Both dashboards include standard navigation links like "CloudShell", "Feedback", "Privacy", "Terms", and "Cookie preferences". The bottom status bar shows system information including battery level, signal strength, and the date/time (30-01-2025).

PROJECT 11

Create IAM policies inheritance for your company

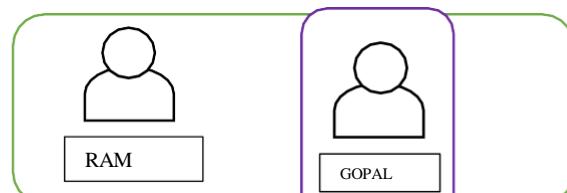


Group:developers

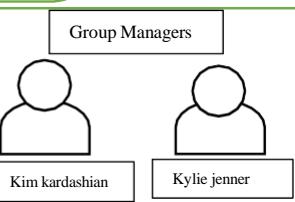
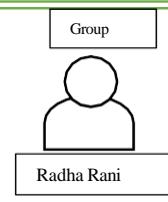
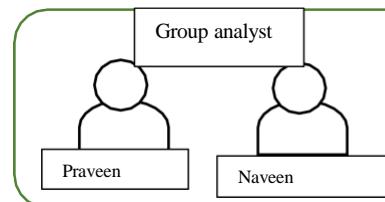
Group:operators

Group:audit team

Group:cloud engineers

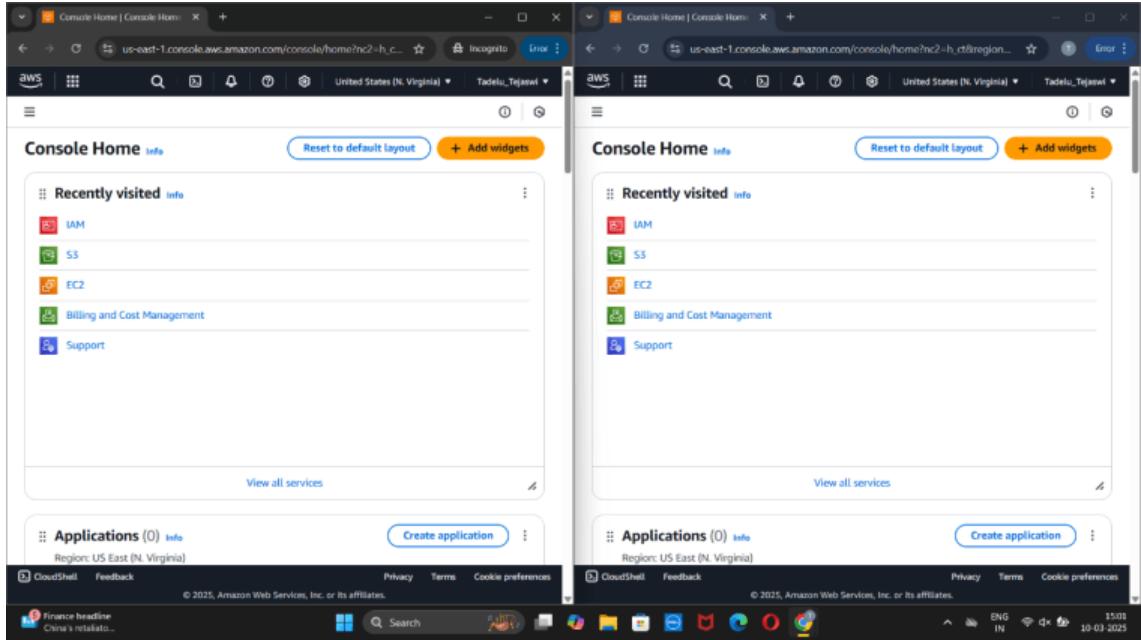


developers

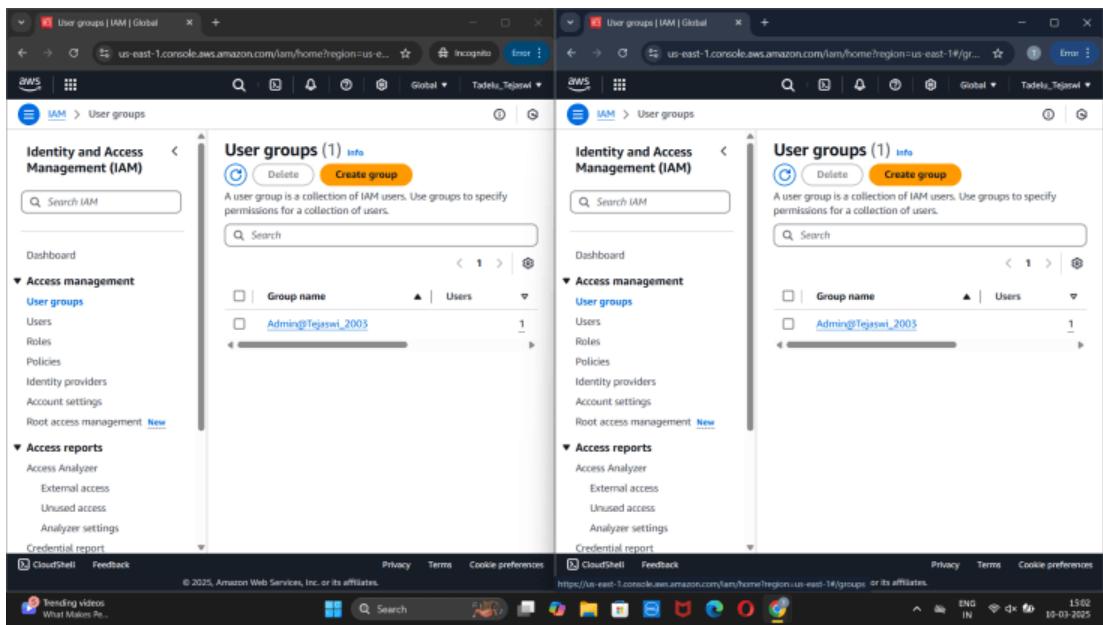


Project-12

- Remove the permissions for a specific user in IAM
Step 1:- Open console home in two different tabs



Step 2:-Now click on IAM users, select the AWS account that has the user you want to remove



The image displays two side-by-side screenshots of the AWS Identity and Access Management (IAM) console. Both screenshots show the 'Permissions' tab for different user groups.

Screenshot 1 (Left): Shows the 'Permissions' tab for the user group 'Admin@Tejaswi_2003'. It lists one policy named 'AmazonSSMManagedInstanceCore'. The policy details are as follows:

- Policy name:** Admin@Tejaswi_2003
- Creation date:** January 22, 2025, 13:17 (UTC-05:00)
- ARN:** arn:aws:iam::841162000:policy/Admin@Tejaswi_2003
- Description:** This policy allows the user Admin@Tejaswi_2003 to manage AWS Lambda functions.

Screenshot 2 (Right): Shows the 'Permissions' tab for the user group 'Admin@Tejaswi_2003'. It lists one policy named 'AmazonSSMManagedInstanceCore'. The policy details are as follows:

- Policy name:** Admin@Tejaswi_2003
- Creation date:** January 22, 2025, 13:17 (UTC-05:00)
- ARN:** arn:aws:iam::841162000:policy/Admin@Tejaswi_2003
- Description:** This policy allows the user Admin@Tejaswi_2003 to manage AWS Lambda functions.

Step 3:-Select multi-account permission

The image displays two side-by-side screenshots of the AWS IAM console, similar to the ones above, but with a specific policy highlighted.

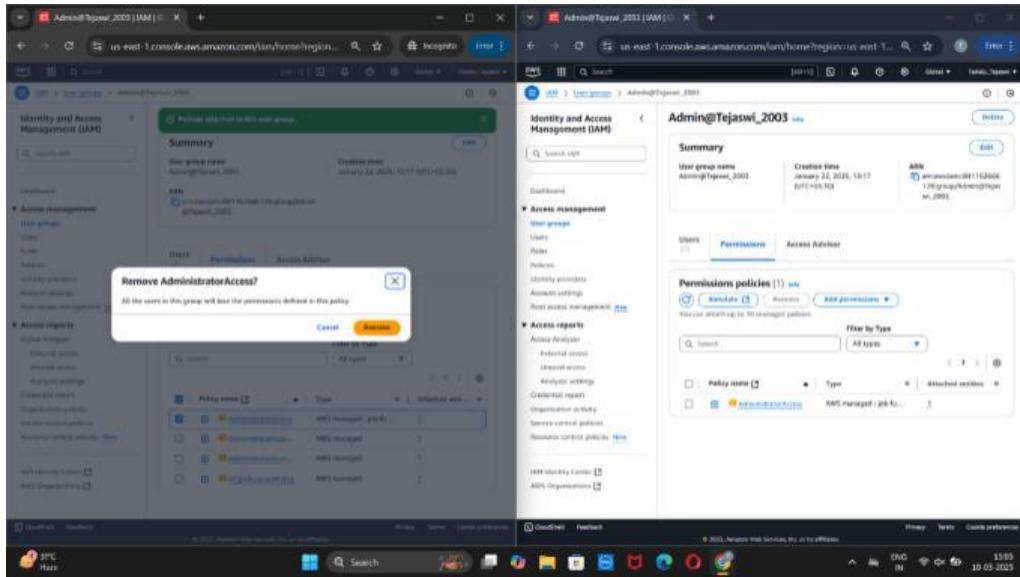
Screenshot 1 (Left): Shows the 'Permissions' tab for the user group 'Admin@Tejaswi_2003'. It lists four policies:

- AmazonSSMManagedInstanceCore** (selected)
- AmazonSSMManagedInstanceCore**
- AmazonSSMManagedInstanceCore**
- AmazonSSMManagedInstanceCore**

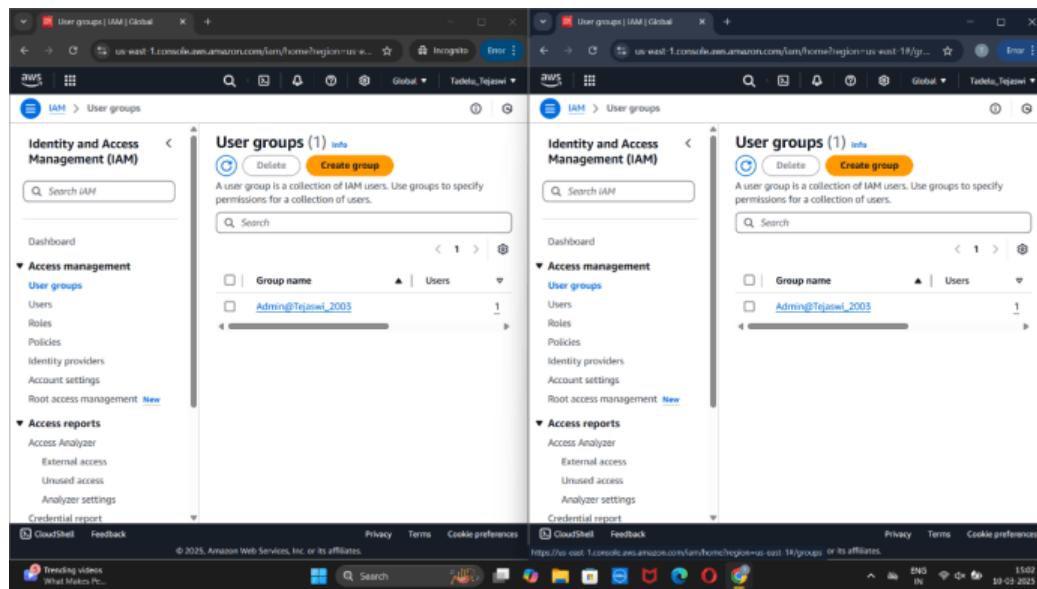
Screenshot 2 (Right): Shows the 'Permissions' tab for the user group 'Admin@Tejaswi_2003'. It lists four policies:

- AmazonSSMManagedInstanceCore** (selected)
- AmazonSSMManagedInstanceCore**
- AmazonSSMManagedInstanceCore**
- AmazonSSMManagedInstanceCore**

Step 4:-Choose the AWS account, select the name of the user you want to remove



Step 5:- Confirm the names of the users in the dialog box, Choose the remove access



Step 6:-Choose the remove access again

The screenshot shows the AWS Identity and Access Management (IAM) console with two user groups displayed in separate tabs:

- Admins User Group:** Summary page. Contains one policy: `AdministratorAccess`. Created by `Admin@Tejaswi_2005` on `January 21, 2025, 16:17:01+08:00`.
- Developers User Group:** Summary page. Contains two policies: `AdministratorAccess` and `AmazonCloudWatchLogsFullAccess`. Created by `Admin@Tejaswi_2005` on `January 21, 2025, 16:17:01+08:00`.

Both groups have the `AdministratorAccess` policy attached. The Developers group also has the `AmazonCloudWatchLogsFullAccess` policy attached.

Project 13

Create a password policy

Step 1: Click on Account settings

The screenshot shows the 'Account settings' page in the AWS IAM console. The left sidebar is collapsed. The main content area displays the 'Password policy' section. It states: 'This AWS account uses the following default password policy: Password minimum length: 8 characters'. Below this, under 'Password strength', it says: 'Include a minimum of three of the following mix of character types: Uppercase, Lowercase, Numbers, Non-alphanumeric characters'. To the right, under 'Other requirements', there are two items: 'Never expire password' and 'Must not be identical to your AWS account name or email address'. At the bottom of the page, there is a 'Endpoints [18]' section with a link to 'Edit password policy'.

Step 2: Click on edit

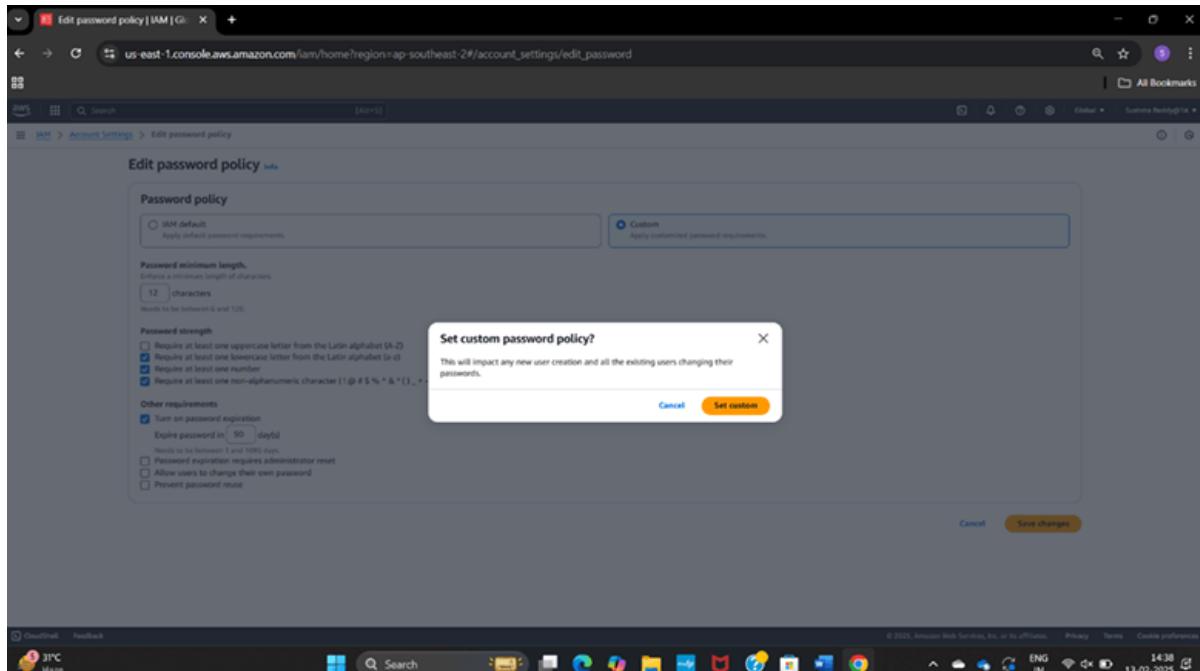
The screenshot shows the 'Edit password policy' dialog box. At the top, there are two radio button options: 'IAM default' (selected) and 'Custom'. The 'IAM default' option has a note: 'Apply default password requirements.' The 'Custom' option has a note: 'Apply customized password requirements.' Below these are sections for 'Password minimum length' (set to 8 characters), 'Password strength' (same requirements as the default policy), and 'Other requirements' (same items as the default policy). At the bottom right of the dialog box are 'Cancel' and 'Save changes' buttons.

Step 3: Click on custom to change password according to you

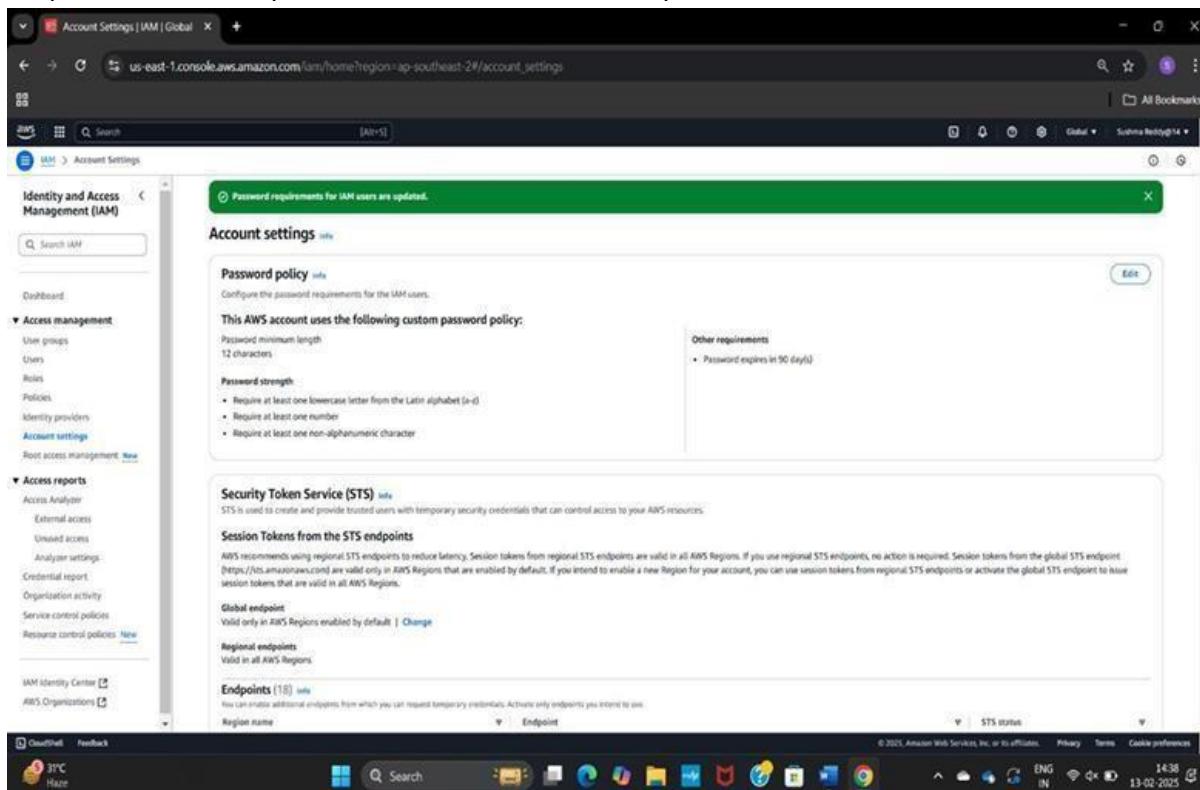
The screenshot shows the 'Edit password policy' page in the AWS IAM console. The 'Custom' tab is selected, indicating 'Apply customized password requirements'. Under 'Password minimum length', a value of '12' is set. In the 'Password strength' section, several requirements are checked: 'Require at least one uppercase letter from the Latin alphabet (A-Z)', 'Require at least one lowercase letter from the Latin alphabet (a-z)', 'Require at least one number', and 'Require at least one non-alphanumeric character (! @ # \$ % ^ & * () _ - + { } []) !)'. Under 'Other requirements', 'Turn on password expiration' is checked, with a note that it will expire in 90 days. Other options like 'Allow users to change their own password' and 'Prevent password reset' are unchecked. At the bottom right are 'Cancel' and 'Save changes' buttons.



Step 4: Select custom password policy



Step 5: Password requirements for IAM users are updated



Project-14

- Login using MFA code

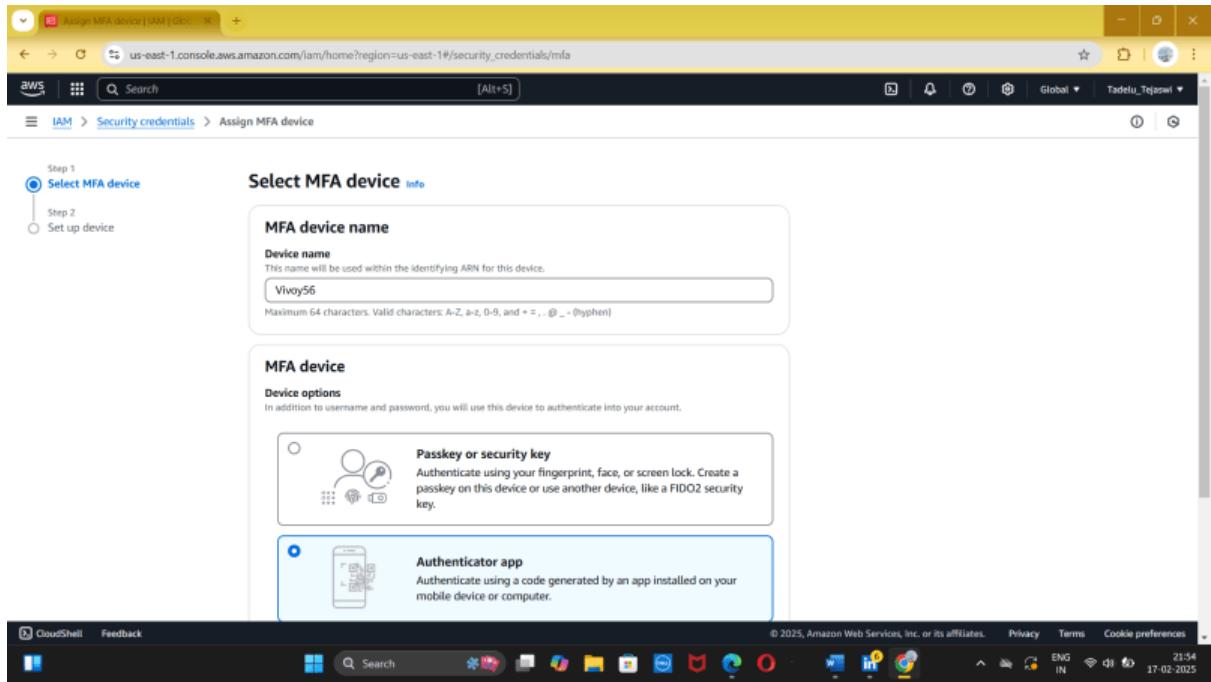
Step 1:-Click on security credentials

The screenshot shows the AWS IAM Account Settings page. On the left, there's a sidebar with options like Identity and Access Management (IAM), Dashboard, Access management, Access reports, and Organization activity. The main content area is titled 'Account settings' and contains sections for 'Password policy' and 'Security Token Service (STS)'. The 'Password policy' section shows a custom policy requiring 12 characters, one lowercase letter, one number, and one non-alphanumeric character. The 'STS' section explains its use for temporary credentials and mentions regional and global endpoints. A right sidebar displays account details such as Account ID (8411-6266-6128), Organization, Service Quotas, Billing and Cost Management, and Security credentials. Buttons for 'Turn on multi-session support' and 'Sign out' are also present.

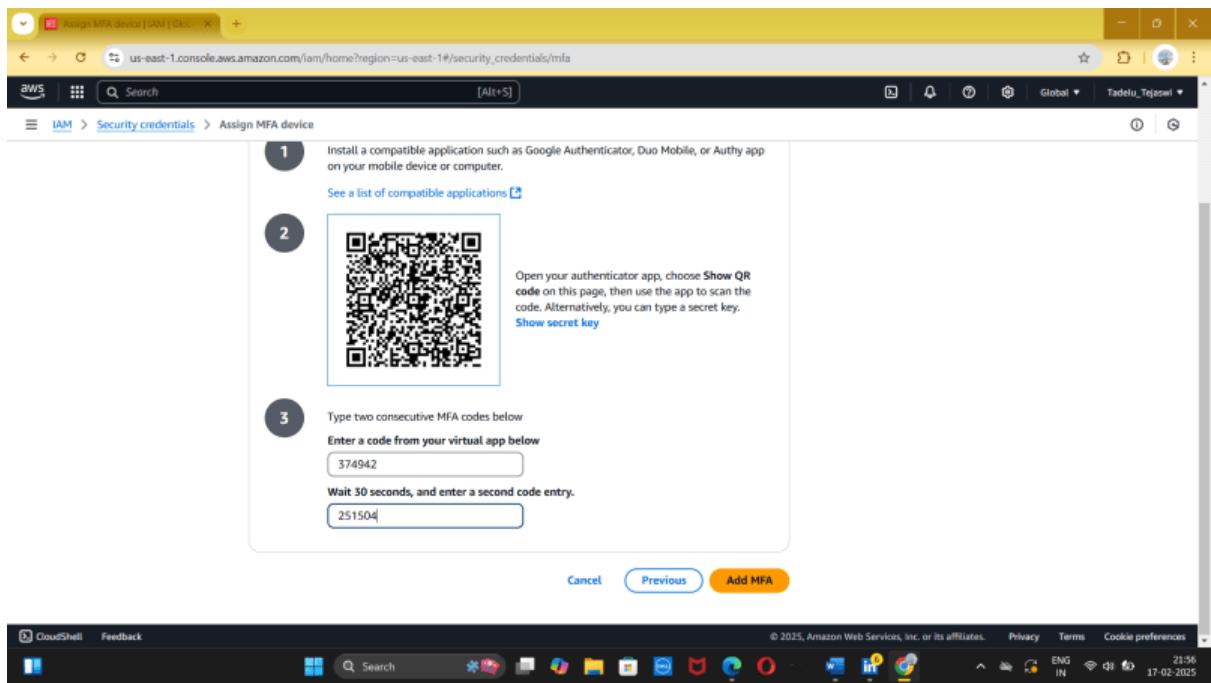
Step 2:-Click on assign MFA

The screenshot shows the AWS IAM Security Credentials page. The sidebar includes options like Identity and Access Management (IAM), Dashboard, Access management, Access reports, and Organization activity. The main content area is titled 'Multi-factor authentication (MFA) (1)' and shows a table with one entry: a virtual device named 'arn:aws:iam::841162666128:mfa/Authapp'. Below this is a section for 'Access keys (0)' with a 'Create access key' button. The bottom of the page includes standard AWS navigation links and a footer with copyright information.

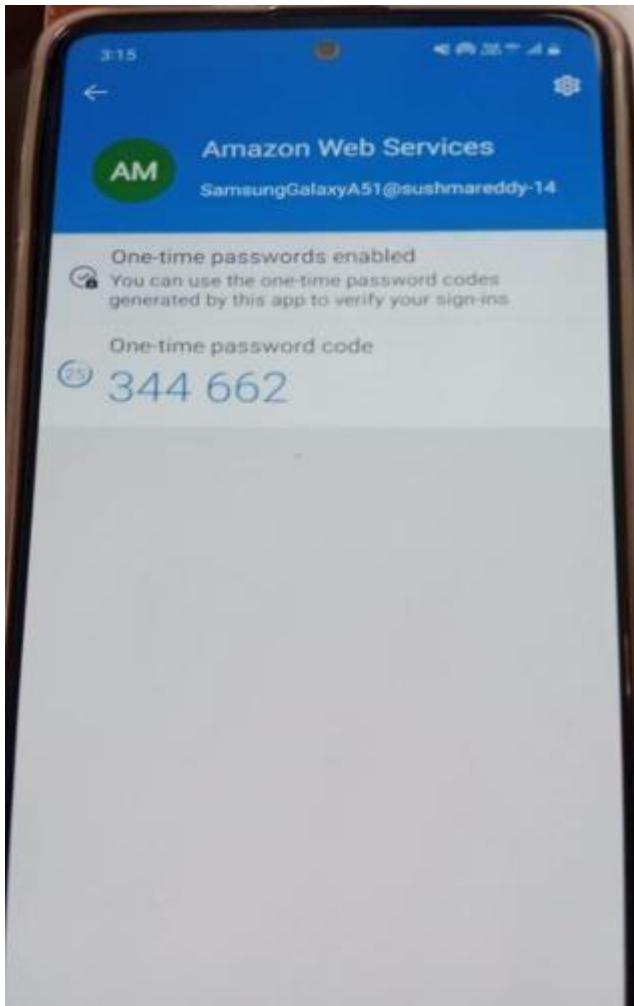
Step 3:- Give the device name and choose Authenticator app



Step 4:- Click on show QR code



Step 5:- Use the authenticator app, you will get two MFA codes. First enter the MFA code 1, then you will receive MFA code 2



Step 6:-MFA device assigned

MFA device assigned

You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.

Multi-factor authentication (MFA) (2)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

Type	Identifier	Certifications	Created on
Virtual	arn:aws:iam::841162666128:mfa/Authapp	Not Applicable	Thu Jan 30 2025
Virtual	arn:aws:iam::841162666128:mfa/Vivo5G	Not Applicable	Mon Feb 17 2025

Create access key

No access keys

As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. [Learn more](#)

Create access key

Step 7:- The device link will be appeared

The screenshot shows the AWS IAM Security Credentials page. A green notification bar at the top states: "MFA device assigned. You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user." Below this, the "Multi-factor authentication (MFA) (2)" section lists two virtual MFA devices. The first device, "amawsiam:841162666128:mfa/Authapp", was created on Jan 30, 2025, and the second, "amawsiam:841162666128:mfa/Vivo5G", was created on Feb 17, 2025. The "Access keys (0)" section indicates no access keys have been created. The bottom of the page includes standard AWS navigation links like CloudShell, Feedback, and a footer with copyright information and status icons.

Step 8:-Now sign out and sign in again

The screenshot shows the AWS sign-in page. A message box at the top says: "Try the new sign in UI. See our new improved Amazon Web Services sign in experience before we officially launch." There is a link to "Enable new sign in". The main form asks for an email address ("Email address: tadelejane70@gmail.com") and an MFA code ("MFA code: 407364"). A "Submit" button is present. To the right, there is a promotional banner for "AWS re:Invent" with the text: "The next generation of Amazon SageMaker is the center for all your data, analytics, and AI." The bottom of the page shows the Windows taskbar with various pinned icons and system status indicators.

Step 9:- Your console home page will be opened

Screenshot of the AWS Console Home page (us-east-1.console.aws.amazon.com) showing various service widgets and navigation.

Recently visited:

- IAM
- Billing and Cost Management
- Support

Applications (0) Info Create application

Region: US East (N. Virginia)

us-east-1 (Current Region) Find applications

No applications
Get started by creating an application. Create application

Welcome to AWS Getting started with AWS Fargate

AWS Health Info Open issues

Cost and usage Info

Current month costs Data unavailable Cost breakdown Data unavailable

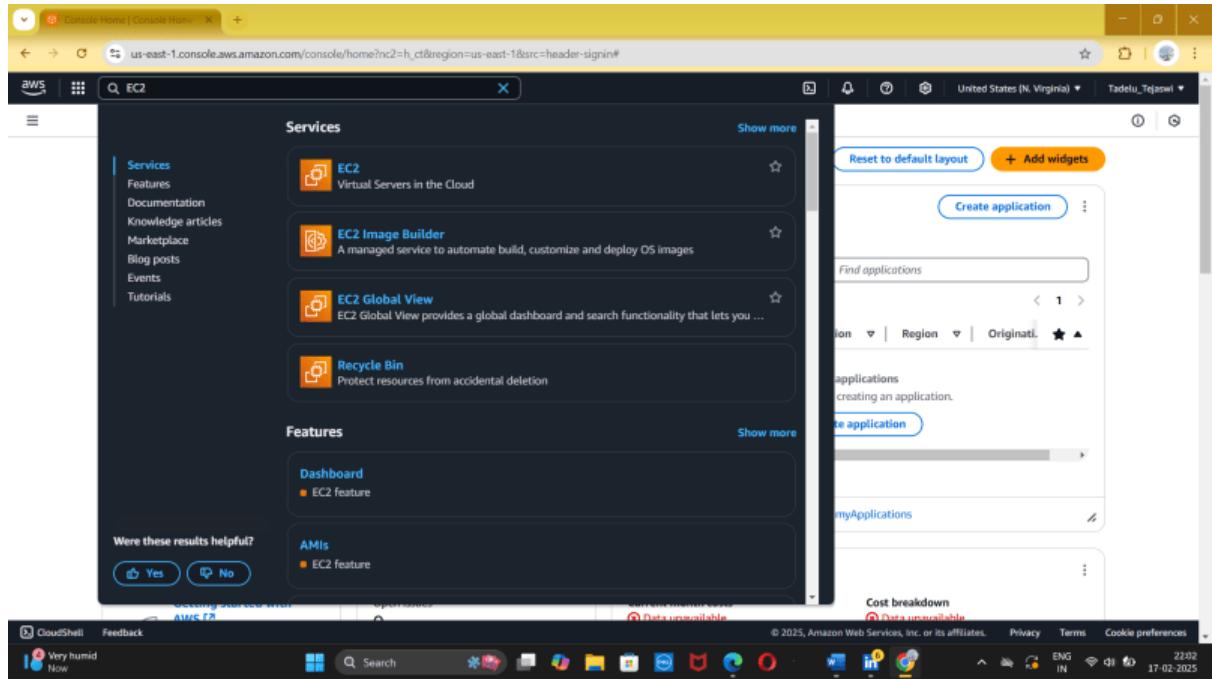
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

CloudShell Feedback Very humid Now ENG IN 23:01 17-02-2025

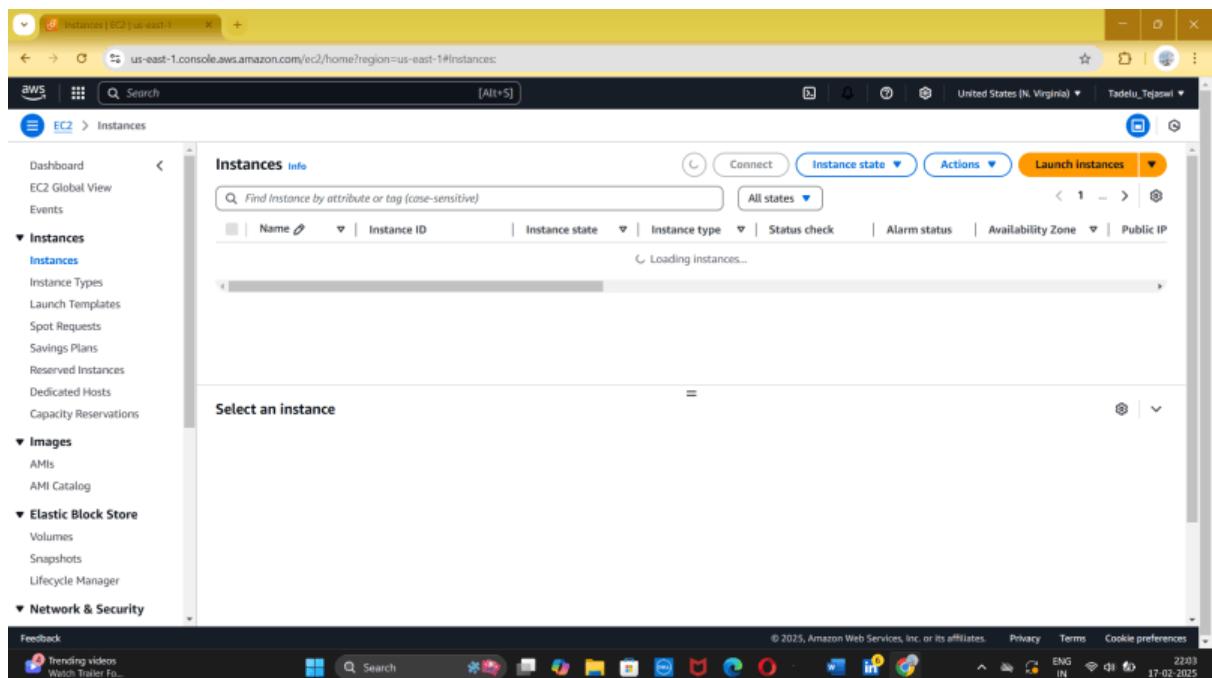
Project-15

- Elastic Compute Cloud (EC2)

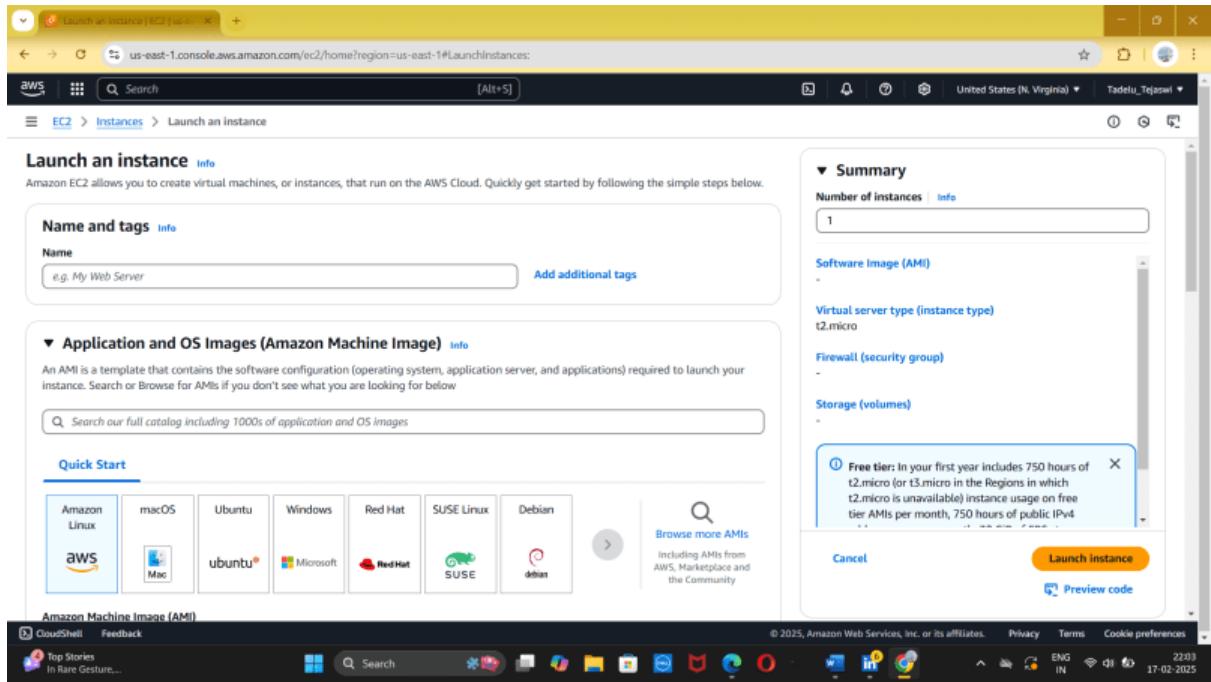
Step 1:-Search EC2 in the console page



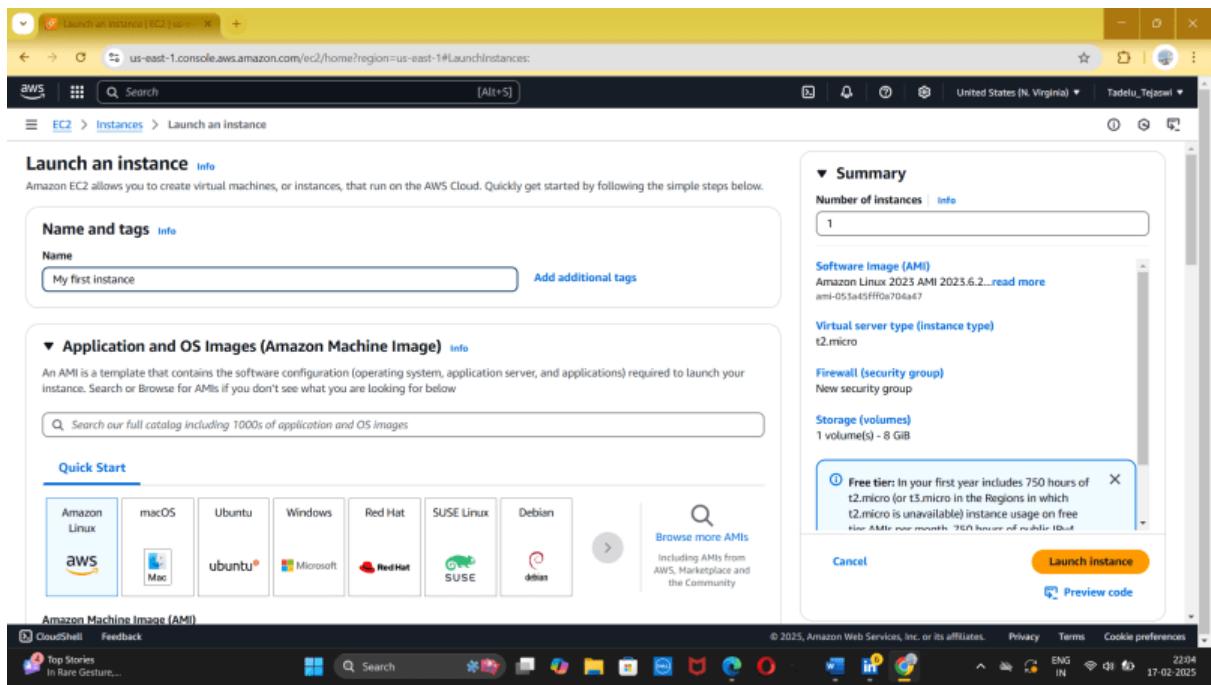
Step 2:- Click on Instance



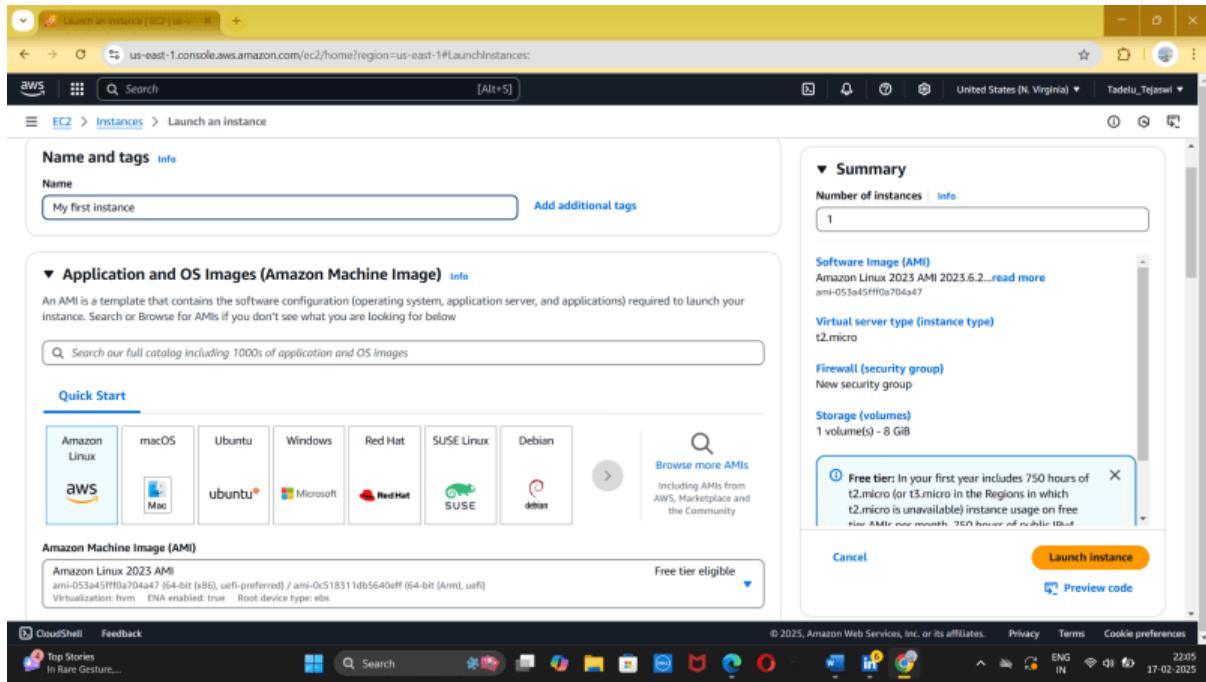
Step 3:- Click on launch instance



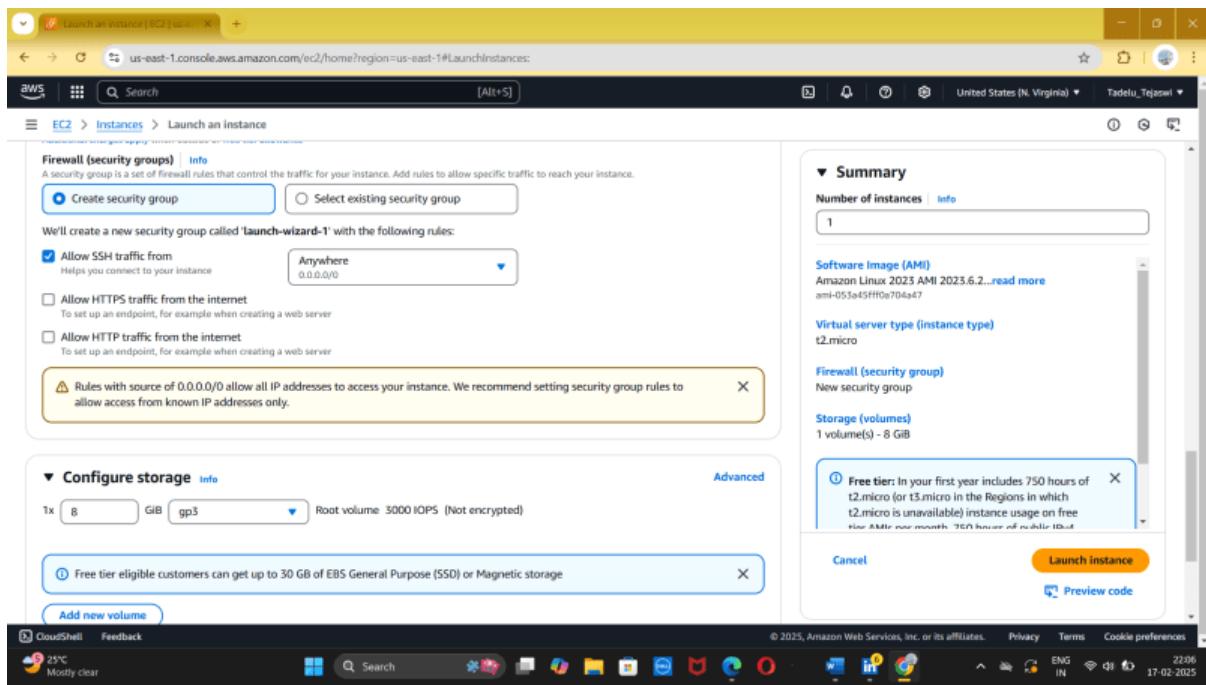
Step 4:- Define Name



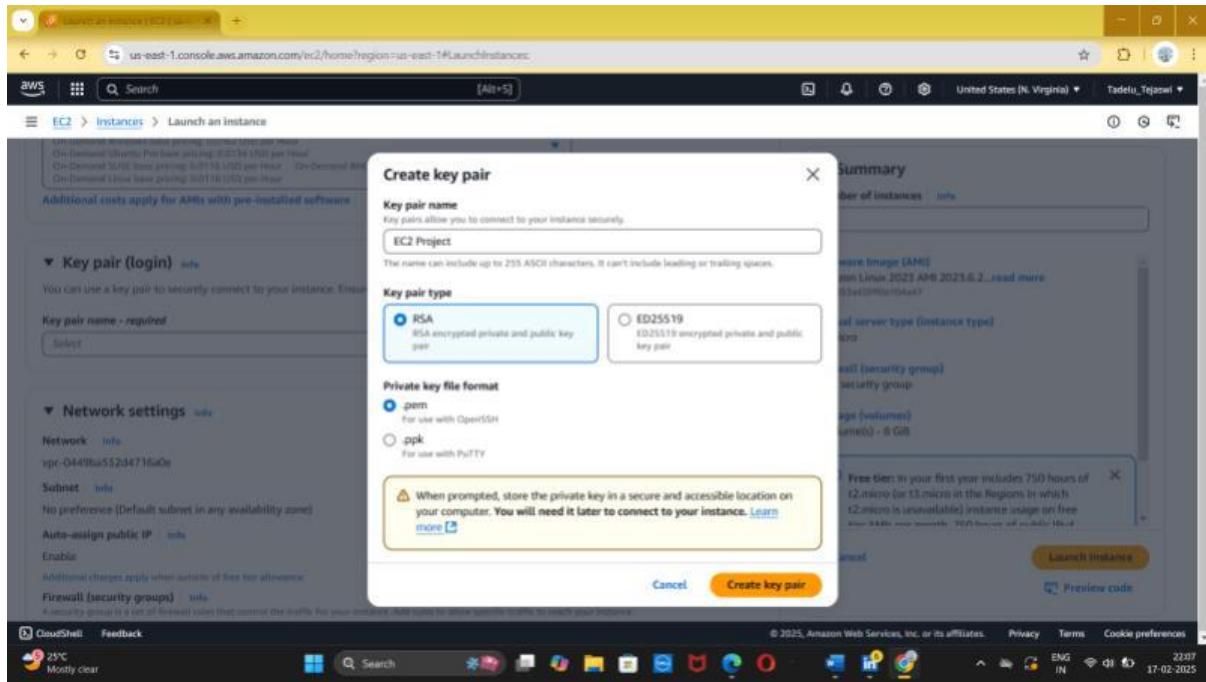
Step 5:- Choose Amazon Linux



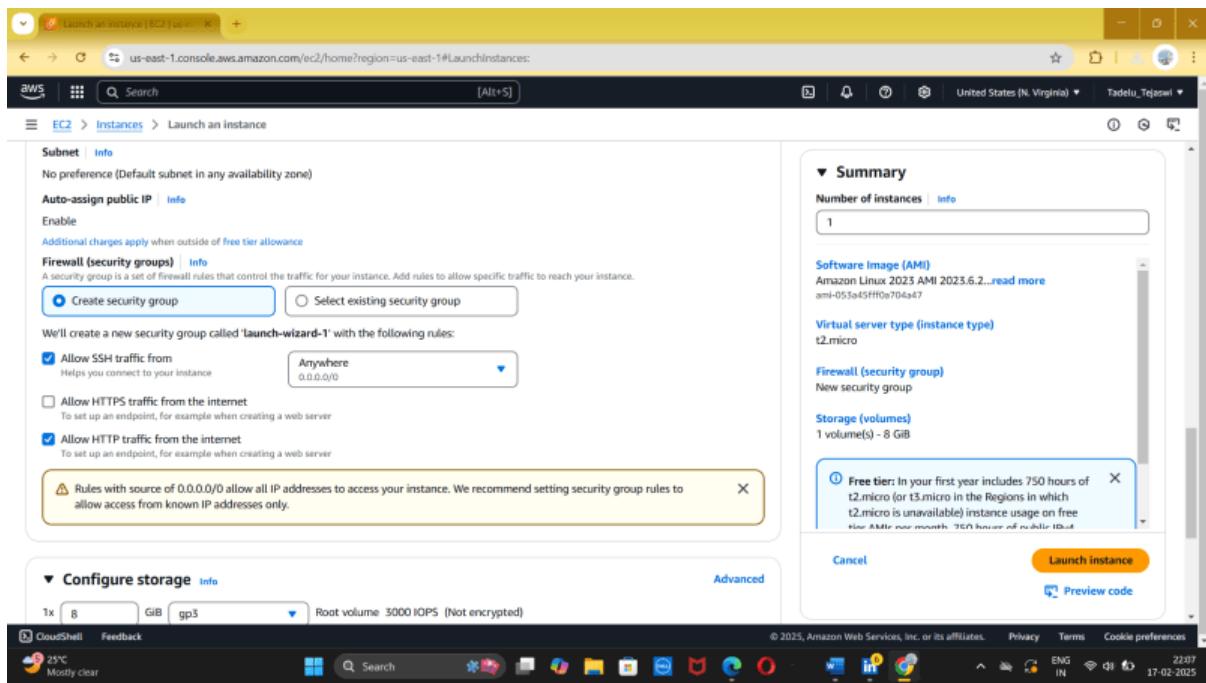
Step 6:-Choose instance type



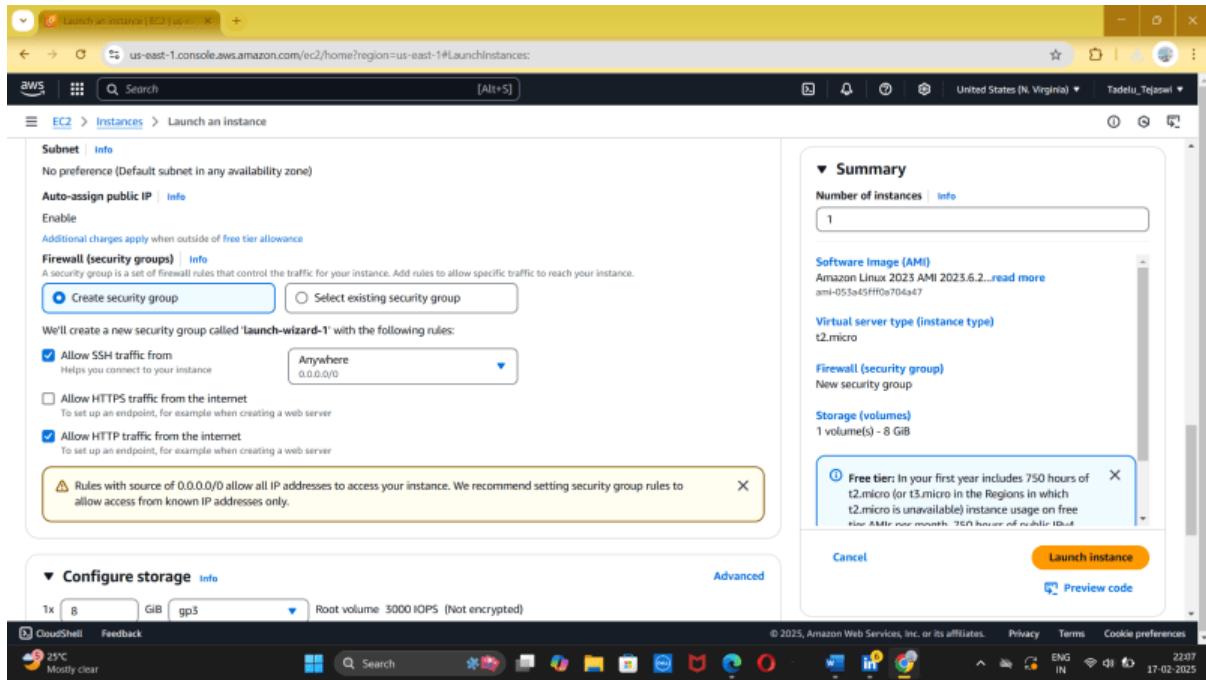
Step 7:-Click on create new key pair and define key pair name and click on create key pair



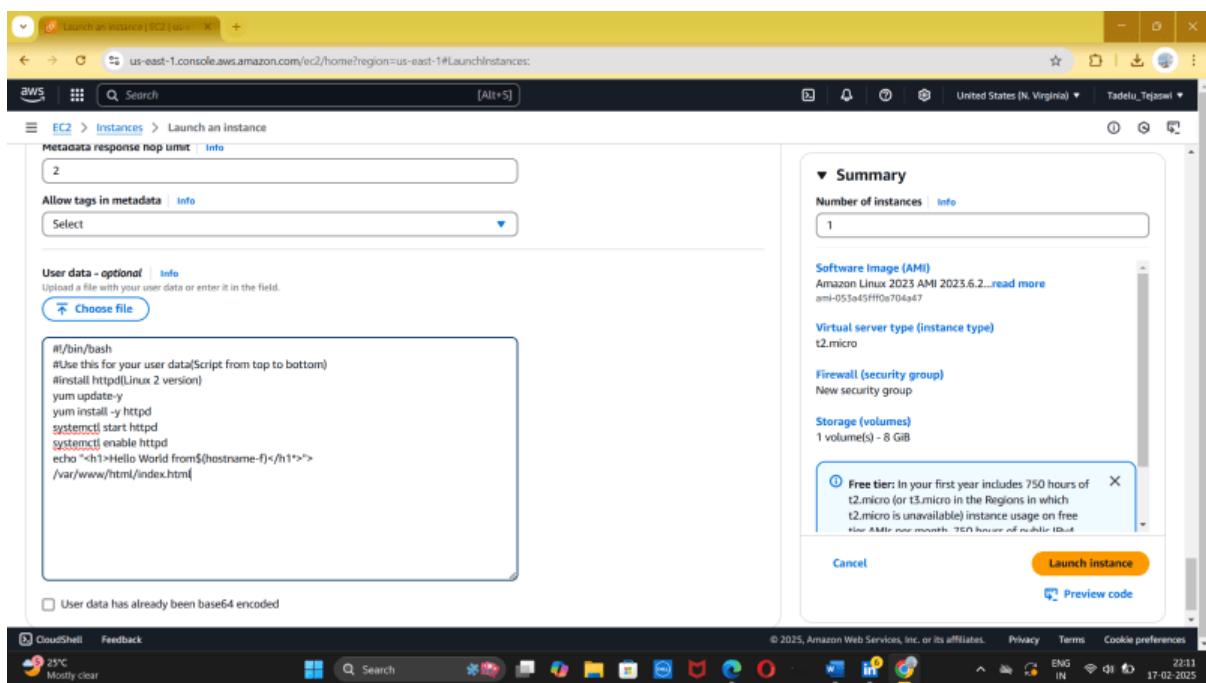
Step 8:-In the Network settings, Select allow SSH ana Http



Step 9:- Have a look on configure storage



Step 10:-Click on Advanced Details and write the code. Now have a look on summary and click on Launch instance



```

#!/bin/bash

# Use this for your user data (script from top to bottom)

# Install httpd (Linux 2 version)

Yum update -y

Yum install -y httpd

Systemctl start httpd

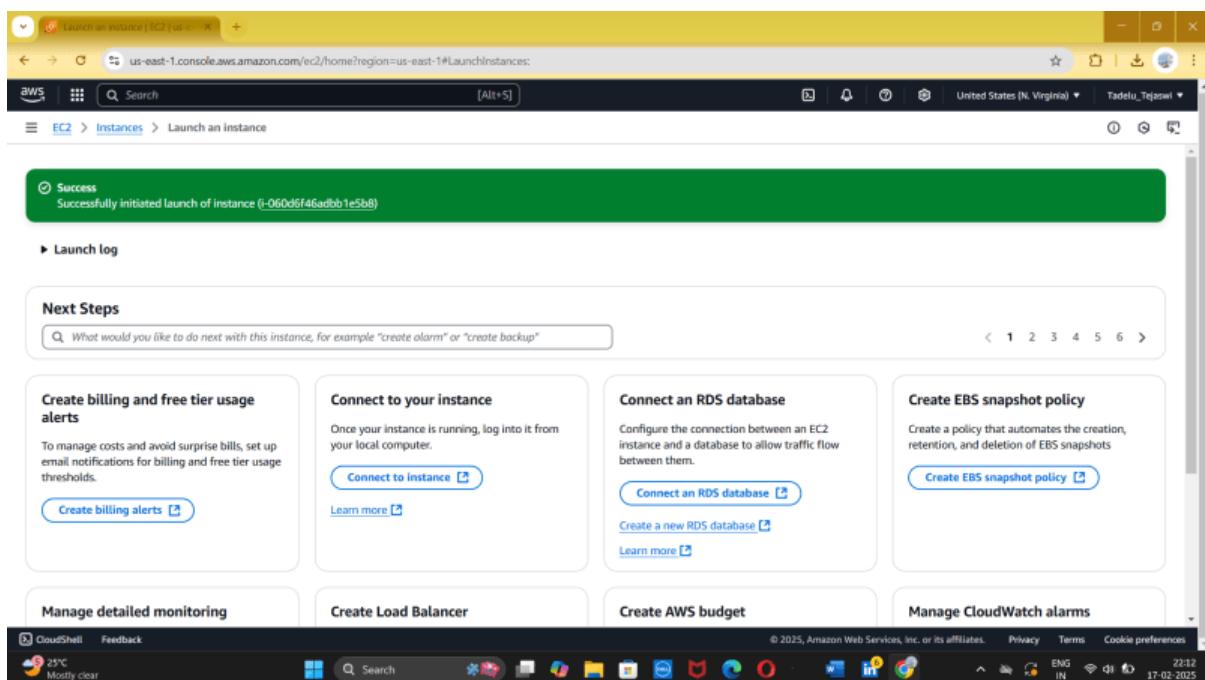
Systemctl enable httpd

Echo "<h1>Hello World from $(hostname-f) </h3>

/var/www/html/index.html

```

Step 11:-Successfully instance will be launched



Step 12:-Now click on instance and check your first instance, it take 30 seconds to update. Please wait and refresh the page, we can see its running

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with sections like Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, and Network & Security. The main content area has tabs for Instances (1) and Info. It shows a table with one row for 'My first instance'. The columns include Name (My first instance), Instance ID (i-060d6f46adb1e5b8), Instance state (Running), Instance type (t2.micro), Status check (Initializing), Alarm status (View alarms), Availability Zone (us-east-1a), and Public IP (ec2-18-2). There are also 'Connect', 'Actions', and 'Launch instances' buttons at the top right.

Step 13:- Click on my first instance and you can see the details down

This screenshot shows the same EC2 Instances page as before, but now the 'My first instance' row is selected. The main content area displays detailed information for this specific instance. At the top, it says 'i-060d6f46adb1e5b8 (My first instance)'. Below that, there are tabs for Details, Status and alarms, Monitoring, Security, Networking, Storage, and Tags. The Details tab is selected. Under 'Instance summary', it shows the Instance ID (i-060d6f46adb1e5b8), Public IPv4 address (18.206.168.129), Private IPv4 address (172.31.17.186), Instance state (Running), and Public IPv4 DNS (ec2-18-206-168-129.compute-1.amazonaws.com). There are also sections for Status and alarms, Monitoring, Security, Networking, Storage, and Tags.

Step 14:-Copy the public IP Address

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with options like Dashboard, EC2 Global View, Instances, Images, Elastic Block Store, and Network & Security. The main area displays a table of instances. One instance is selected, showing its details. The instance has the following attributes:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
My first instance	i-060d6f46adbb1e5b8	Running	t2.micro	Initializing	View alarms	us-east-1a	ec2-18-2

Below the table, the instance details are shown in a modal window. It includes sections for Instance summary, Details, Status and alarms, Monitoring, Security, Networking, Storage, and Tags. The Public IPv4 address is highlighted: 18.206.168.129.

Step 15:-Paste the URL in the new browser and run it

A screenshot of a browser window. The address bar shows the URL: 18.206.168.129. The page content is mostly blank, indicating that the website at this IP address is not currently active or is under construction.

It works!



Step 16:- Now stop to avoid billing from AWS

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with options like Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, and Network & Security. The main content area shows a table of instances. One instance, with the ID i-060d6f46adb1e5b8 and the name 'My first instance', is selected and highlighted in blue. A context menu is open over this instance, with 'Stop instance' being the selected option. Other options in the menu include Start instance, Reboot instance, Hibernate instance, and Terminate (delete) instance. The instance details page for 'My first instance' is also visible, showing its public and private IP addresses, instance state (Running), and other configuration details.

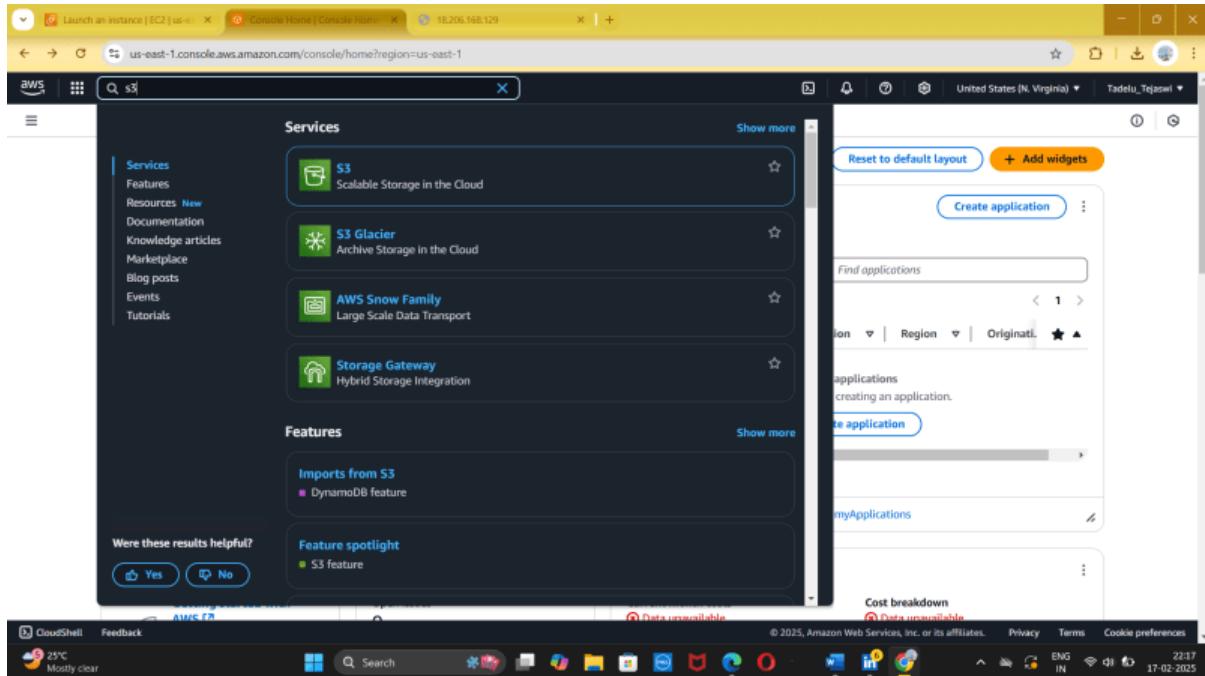
Step 17:- Successfully stopped.

This screenshot shows the same AWS EC2 Instances page after the instance has been stopped. The green success message at the top of the page reads "Successfully initiated stopping of i-060d6f46adb1e5b8". The instance table now shows the instance in the 'Initializing' state. The instance details page for 'My first instance' is still visible, showing its public and private IP addresses, instance state (Running), and other configuration details.

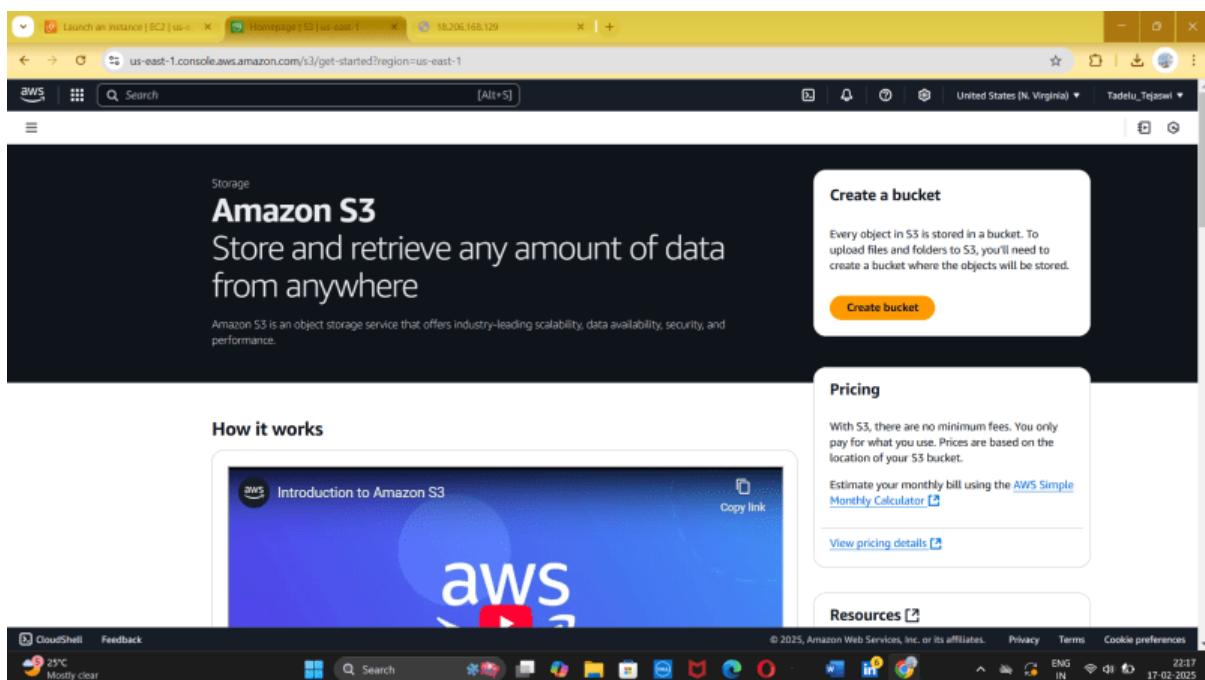
Project-16

- Creating of S3 Buckets and Objects

Step 1:-Search S3 in the console home page



Step 2:- Click on create object



Step 3:-Define AWS Region and Bucket name

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region: US East (N. Virginia) us-east-1

Bucket type: [Info](#)

General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

Directory
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name: [Info](#)
myawsbucket

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Format: s3://bucket/prefix

Object Ownership [Info](#)

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 23:18 ENG IN 17-02-2025

Step 4:- Have a look on default settings and click on create Bucket.

Tags - optional (0)
You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

[Add tag](#)

Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type: [Info](#)

Server-side encryption with Amazon S3 managed keys (SSE-S3)
 Server-side encryption with AWS Key Management Service keys (SSE-KMS)
 Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the Storage tab of the [Amazon S3 pricing page](#).

Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

Disable
 Enable

Advanced settings

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 23:19 ENG IN 17-02-2025

Step 5:-Successfully bucket will be created

The screenshot shows the AWS S3 console with a green success message at the top: "Successfully created bucket 'myawsbucket232355'. To upload files and folders, or to configure additional bucket settings, choose View details." Below this, there's an "Account snapshot" section with a link to "View Storage Lens dashboard". Under "General purpose buckets", there is one entry: "myawsbucket232355" (US East (N. Virginia) us-east-1). There are buttons for "Copy ARN", "Empty", "Delete", and "Create bucket".

The screenshot shows a Windows taskbar with various icons, including the AWS CloudShell icon.

Step 6:- Click on your bucket

The screenshot shows the "Objects" tab of the AWS S3 console for the "myawsbucket232355" bucket. It displays a message: "No objects. You don't have any objects in this bucket." There is a "Upload" button at the bottom.

The screenshot shows a Windows taskbar with various icons, including the AWS CloudShell icon.

Step 7:- 0 objects will be appeared

The screenshot shows the AWS S3 console interface. At the top, there are three tabs: 'Launch an instance | EC2 | us-east-1', 'myawsbucket232355 | S3 Buckets', and '18.206.168.129'. Below the tabs, the URL is 'us-east-1.console.aws.amazon.com/s3/buckets/myawsbucket232355?region=us-east-1&bucketType=general&tab=objects'. The main navigation bar includes 'Amazon S3 > Buckets > myawsbucket232355'. The page title is 'myawsbucket232355 Info'. A horizontal menu bar at the top of the content area includes 'Objects', 'Metadata', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. The 'Objects' tab is selected. Below this, a sub-menu bar includes 'Actions', 'Create folder', and 'Upload'. A search bar labeled 'Find objects by prefix' is present. The main content area displays a message: 'No objects' and 'You don't have any objects in this bucket.' There is a blue 'Upload' button at the bottom.

The screenshot shows a Windows taskbar with several application icons visible, including CloudShell, Feedback, Weather (25°C), Search, File Explorer, and others. The system tray shows the date (17-02-2025) and time (22:21). The status bar at the bottom indicates the language is ENG IN.

Step 8:- Click on upload. Click on upload object and click on upload

The screenshot shows the AWS S3 console interface for the 'Upload' step. The URL is 'us-east-1.console.aws.amazon.com/s3/upload/myawsbucket232355?region=us-east-1&bucketType=general'. The main content area has a heading 'Upload Info' with a sub-instruction: 'Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. Learn more'. Below this is a large blue rectangular area with the text 'Drag and drop files and folders you want to upload here, or choose Add files or Add folder.' A 'Files and folders (0)' section follows, with a sub-instruction: 'All files and folders in this table will be uploaded.' It includes a search bar 'Find by name' and a table header with columns 'Name', 'Folder', 'Type', and 'Size'. The message 'No files or folders' is displayed. The 'Destination' section is shown next, with the URL 's3://myawsbucket232355'. A 'Destination details' link is present. The bottom of the screen shows the same Windows taskbar and system tray as the previous screenshot.

Step 9: Successfully will be uploaded

The screenshot shows the AWS S3 'Upload objects' page. A green success message at the top states: 'Upload succeeded. For more information, see the Files and folders table.' Below this, a summary table shows 'Succeeded' (1 file, 54.5 KB) and 'Failed' (0 files, 0 B). The 'Files and folders' tab is selected, displaying a table with one row: 'rbphoto.jpg' (image/jpeg, 54.5 KB, Succeeded). The browser's address bar shows the URL: 'us-east-1.console.aws.amazon.com/s3/upload/myawsbucket232355?region=us-east-1&bucketType=general'.

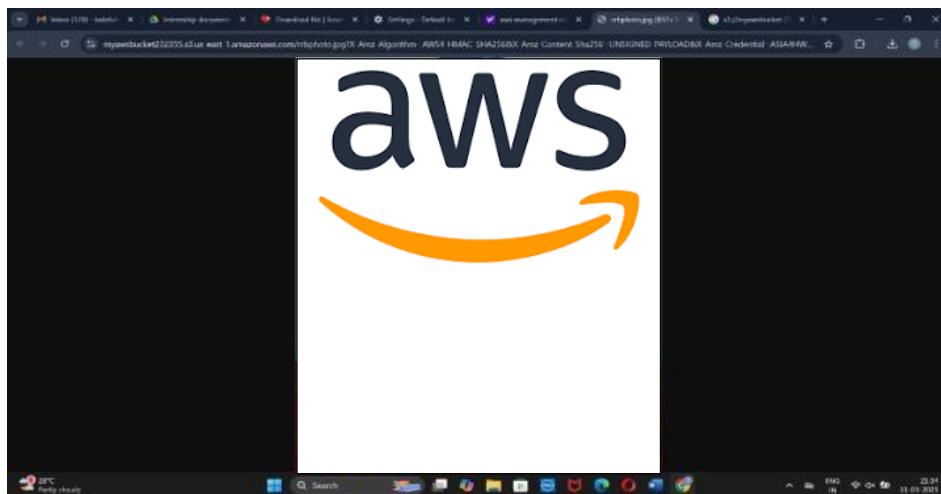
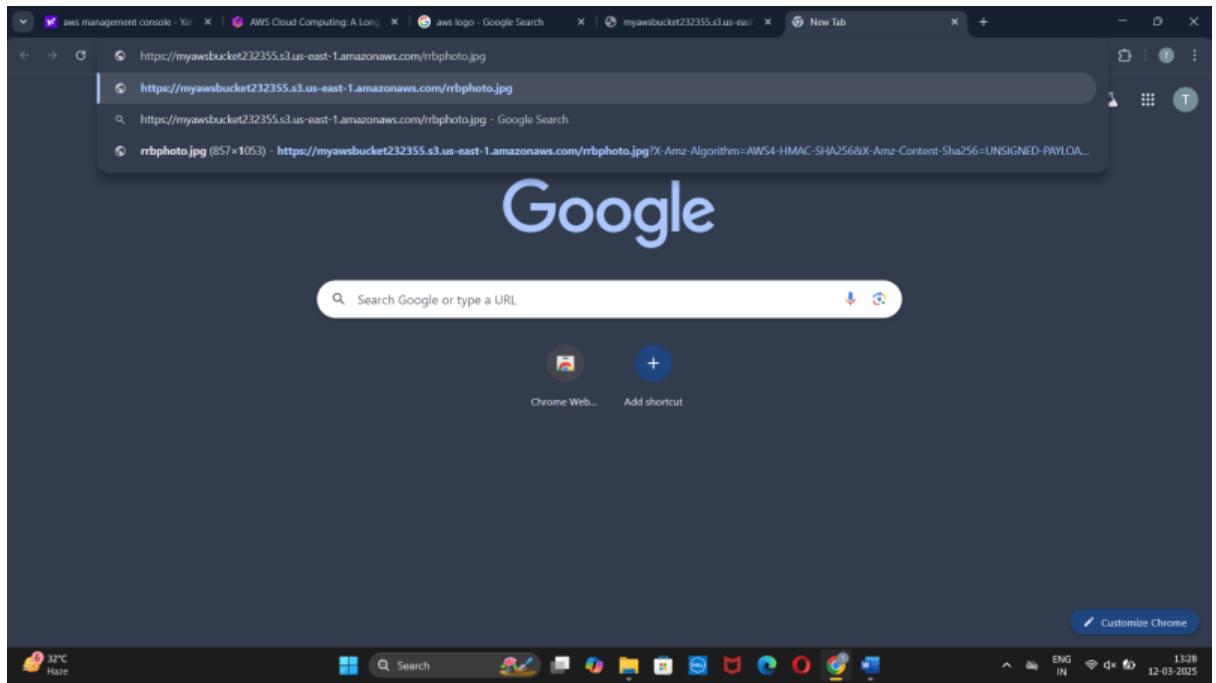
Step 10: Go to objects and click on the object you have created

The screenshot shows the AWS S3 'Objects' list for the 'myawsbucket232355' bucket. The left sidebar shows various AWS services like Lambda, CloudWatch Metrics, and Storage Lens. The main area displays a table with one row: 'rbphoto.jpg' (image/jpeg, 54.5 KB, Standard storage class). The object is selected, indicated by a blue border around its row. The browser's address bar shows the URL: 'us-east-1.console.aws.amazon.com/s3/buckets/myawsbucket232355?region=us-east-1&bucketType=general&tab=objects'.

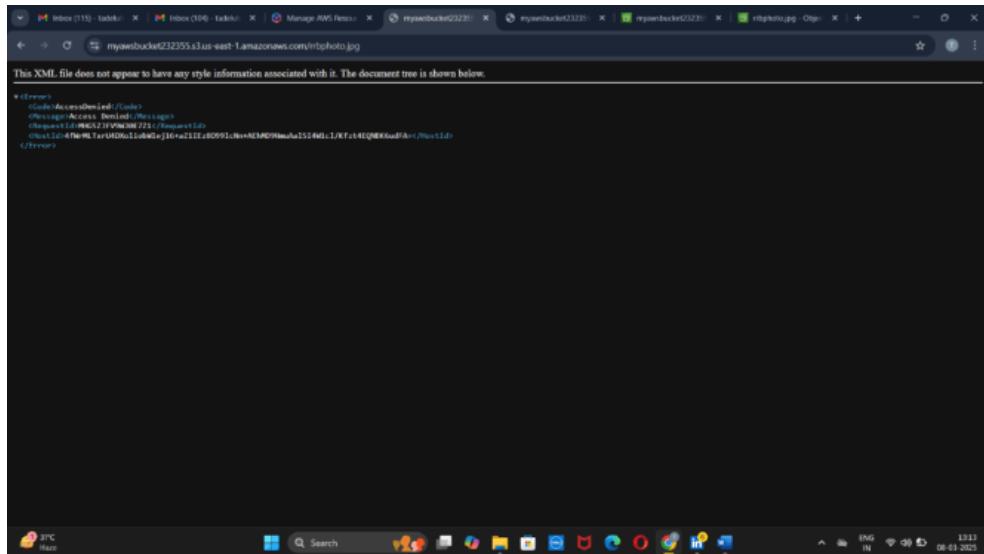
Step 11:- Object details will be overviewed and click on open

The screenshot shows the AWS S3 'Object details' page for 'rbphoto.jpg'. The left sidebar shows the bucket structure. The main area has tabs for 'Properties', 'Permissions', and 'Versions'. The 'Properties' tab is selected, showing details like 'Name: rbphoto.jpg', 'Last modified: Mon, 08 May 2023 15:38:51 UTC', and 'Size: 54.5 KB'. Below this is the 'Object management overview' section, which includes 'Bucket Versioning' (disabled), 'Replication status' (disabled), and 'Expiration rule' (disabled). The browser's address bar shows the URL: 'us-east-1.console.aws.amazon.com/s3/object/myawsbucket232355/rbphoto.jpg'.

Step 12:-Copy the URL and open it



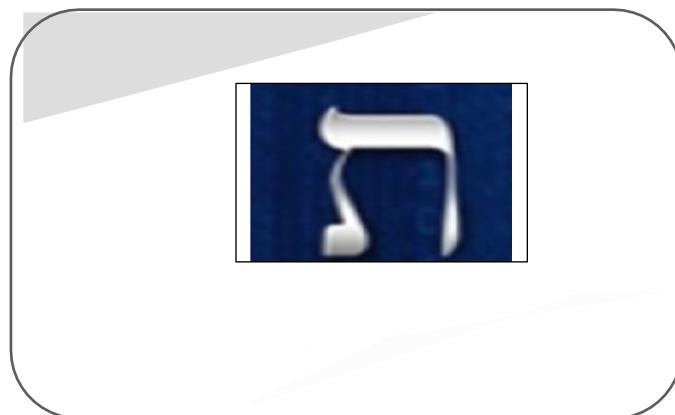
Step 13:- Object denied





ADHOC NETWORK TECH, VIZAG

ADITYA DEGREE COLLEGE, RAMNAGAR(LONG TERM INTERNSHIP)



RESTRICT EC2 ACTIONS USING IAM POLICIES

MINI PROJECT-1

TEAM MEMBERS

T.Tejaswi

D.Tejaswini

K.chinmayi

M.sravanthi

K.vijaya joytha

MARCH 7, 2025
ADHOC NETWORK TECH
VISAKHAPATNAM

INTRODUCTION

In cloud environments, managing permissions effectively is crucial to ensuring security and operational efficiency. AWS Identity and Access Management (IAM) allows fine-grained control over user actions. This project focuses on creating an IAM policy to restrict EC2 instance actions—permitting users to start and stop instances while preventing them from terminating any. This ensures operational flexibility without the risk of accidental or unauthorized instance deletion.

By implementing this policy, organizations can enforce better governance, protect critical workloads, and minimize accidental disruptions while still allowing necessary instance management operations.

Cloud security is a key aspect of managing AWS resources effectively. AWS Identity and Access Management (IAM) enables administrators to define fine-grained permissions for users and roles. In this project, we will create an IAM policy that restricts EC2 instance actions—allowing users to start and stop instances but preventing them from terminating them.

This restriction is crucial for maintaining operational stability, preventing accidental data loss, and enforcing governance policies in an AWS environment. By implementing this policy, organizations can ensure that instances remain protected from unintended deletions while still granting users the flexibility to manage compute resources as needed. This approach enhances security, reduces downtime risks, and aligns with best practices in cloud management.

Additionally, this policy can be customized to include more granular permissions based on specific user roles and responsibilities. For instance, administrators may allow developers to restart instances but restrict modifications to instance configurations or security groups. This ensures that users have only the necessary permissions required for their tasks, reducing the risk of misconfigurations or unauthorized changes.

Implementing IAM policies also supports compliance with security standards and organizational policies. Many industries require strict access control to prevent unauthorized resource modifications. By restricting EC2 instance termination, businesses can align their cloud security strategies with best practices, ensuring accountability and reducing potential vulnerabilities.

Furthermore, this policy can be integrated with AWS CloudTrail to monitor and log all user actions related to EC2 instances. This enhances transparency and provides insights into access patterns, helping organizations audit changes and investigate any unauthorized attempts to terminate instances. Combining IAM policies with logging and monitoring tools strengthens overall cloud governance and security posture.

In conclusion, implementing an IAM policy to restrict EC2 instance termination enhances security, operational stability, and compliance within an AWS environment. It ensures that users can manage instances efficiently without the risk of accidental deletion, safeguarding critical workloads. By combining this policy with monitoring and auditing tools, organizations can strengthen their cloud governance, maintain better control over resource management, and align with industry best practices for security and access control.

ALGORITHM

- Create an IAM Policy:***
 - ***Open the AWS IAM Console.***
 - ***Navigate to Policies and click Create Policy.***
- Define the JSON Policy:***
 - ***Allow ec2: StartInstances and ec2: StopInstances.***
 - ***Deny ec2: TerminateInstances.***
- Attach the Policy to Users/Roles:***
 - ***Go to IAM Users or IAM Roles.***
 - ***Attach the newly created policy to the intended users or roles.***
- Test the Policy:***
 - ***Log in as a user with this policy.***
 - ***Attempt to start, stop, and terminate an EC2 instance.***
 - ***Ensure that termination is blocked while the other actions are allowed.***

MINI PROJECT 1

PROJECT NAME: CREATE A POLICY THAT ALLOWS USERS TO START OR STOP EC2 INSTANCES BUT NOT TERMINATE THEM.

Step 1: Login in to the AWS with Rootuser

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with 'Identity and Access Management (IAM)' and links for 'Dashboard', 'Access management' (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management), 'Access reports' (Access Analyzer, External access, Unused access, Analyzer settings, Credential report, Organization activity), and 'CloudShell' and 'Feedback'. The main area has sections for 'Security recommendations' (Root user has MFA, Root user has no active access keys), 'AWS Account' (Account ID: 841162666128, Account Alias: tejaswi-2345, Sign-in URL: https://tejaswi-2345.sigin.aws.amazon.com/console), 'IAM resources' (Resources in this AWS Account: User groups: 1, Users: 1, Roles: 2, Policies: 0, Identity providers: 0), 'What's new' (Updates for features in IAM: AWS IAM announces support for encrypted SAML assertions, AWS CodeBuild announces support for project ARN and build ARN IAM condition keys, IAM Roles Anywhere credential helper now supports TPM 2.0), and 'Quick Links' (My security credentials, Manage your access keys, multi-factor authentication (MFA) and other credentials). At the bottom, there's a toolbar with various icons and system status indicators.

Step 2: Click on Policies and then Create policy

The screenshot shows the 'Policies' page. The sidebar is identical to the previous dashboard. The main area displays a table titled 'Policies (1335)'. The table has columns for 'Policy name', 'Type', 'Use...', and 'Description'. The first few rows show standard AWS managed policies like 'AccessAnalyzerServiceRolePolicy', 'AdministratorAccess', 'AdministratorAccessPolicy', etc. There are 67 pages of results. At the top right, there are buttons for 'Actions', 'Delete', and 'Create policy'. The bottom of the screen shows the same AWS navigation bar and system status as the previous screenshot.

Step 3: After clicking on create policies then select JSON on tab and enter the code

The screenshot shows the AWS IAM Policy editor interface. The left pane displays the JSON code for a policy:

```
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Action": [
7                  "ec2:StartInstances",
8                  "ec2:StopInstances"
9              ],
10             "Resource": "arn:aws:ec2:*::instance/*"
11         },
12         {
13             "Effect": "Deny",
14             "Action": [
15                 "ec2:TerminateInstances"
16             ],
17             "Resource": "arn:aws:ec2/*::instance/*"
18         }
19     ]
20 }
```

The right pane has tabs for "Visual" (selected), "JSON" (selected), and "Actions". A sidebar on the right says "Edit statement" and "Select a statement". A button at the bottom right says "+ Add new statement". The bottom of the screen shows the Windows taskbar with various icons.

Step 4: After entering the code click on next and give the policy name then click on create policy

The screenshot shows the "Create policy" step of the AWS IAM wizard. The "Policy name" field contains "EC2startStopTerminate". The "Description - optional" field is empty. The "Permissions defined in this policy" section shows two entries:

- Explicit deny (1 of 440 services)**: EC2, Limited Write, InstanceID string like [All], reportString like [All], Request condition: None.
- Allow (1 of 440 services)**: EC2, Limited Write, InstanceID string like [All], reportString like [All], Request condition: None.

The "Add tags - optional" section is empty. At the bottom, there are "Cancel", "Previous", and "Create policy" buttons. The bottom of the screen shows the Windows taskbar.

Step 5: So the policy successfully created

The screenshot shows the AWS IAM Policies page. A green banner at the top indicates that the policy 'EC2startStopNoTerminate' has been created. The main table lists 1336 policies, with the new one being the first item. The table includes columns for Policy name, Type, Used as, and Description. The 'Used as' column shows 'None' for all policies, except for the first one which is 'Permissions policy (1)'. The 'Description' column provides details for each policy, such as 'Allow Access Analyzer to analyze results...' for the first policy.

Policy name	Type	Used as	Description
AccessAnalyzerServiceRolePolicy	AWS managed	None	Allow Access Analyzer to analyze results...
AdministratorAccess	AWS managed - job-function	Permissions policy (1)	Provides full access to AWS services en...
AdministratorAccess-Anglo	AWS managed	None	Grants account administrative permis...
AdministratorAccess-AmazonCloudWatchLogs	AWS managed	None	Grants account administrative permis...
AmazonCloudWatchLogsPolicy	AWS managed	None	Provides CloudWatch permissions require...
AmazonCloudWatchLogsPolicy	AWS managed	None	Grants full access to Amazon CloudW...
AmazonCloudWatchLogsPolicy	AWS managed	None	Grants ReadOnly permissions to the A...
AllowAIOpsSetupAccess	AWS managed	None	Provide dev/test setup access to Alexa...
AllowAIoTBusinessDeviceSetup	AWS managed	None	Provides full access to AlexaForBusiness...
AllowAIoTBossFullAccess	AWS managed	None	Provides full access to AlexaForBusiness...
AllowAIoTBossFullAccess	AWS managed	None	Provide gateway execution access to Al...
AllowAIoTBossFullAccess	AWS managed	None	Provide access to LINQin AWS devices
AllowAIoTBossFullAccess	AWS managed	None	This policy enables Alexa For Business 1...
AllowAIoTBossFullAccess	AWS managed	None	Provide access to Poly AWS devices
AllowAIoTBossFullAccess	AWS managed	None	Provide read only access to AlexaForBu...
AmazonAPIGatewayAdministrator	AWS managed	None	Provides full access to create/edit/Update...
AmazonAPIGatewayInvokeFullAccess	AWS managed	None	Provides full access to invoke APIs in A...
AmazonAPIGatewayPushToCloudWatchlogs	AWS managed	None	Allows API Gateway to push logs to us...

Step 6: Now we have to attach the policy to the Users, So click on users then select the user which you want to attach the policy

The screenshot shows the AWS IAM Users page. It displays a table with one user entry: 'Tjorner@21'. The table includes columns for User name, Path, Group, Last activity, MFA, Password age, Console last sign-in, Access key ID, Active key age, Access key last use, and ARN. The ARN for the user is listed as arn:aws:iam::84116254612:users/Tjorner@21.

User name	Path	Group	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age	Access key last use	ARN
Tjorner@21	/	1	51 days ago		11 days	January 10, 2025, 11:4...	-	-	-	arn:aws:iam::84116254612:users/Tjorner@21

Step 7: After selecting the user Click on Add permissions

The screenshot shows the AWS IAM User Details page for 'Tejaswi@23'. The 'Permissions' tab is selected. Two policies are listed: 'AdministratorAccess' (Attached via Group 'AdministratorGroup') and 'AWSUserChangePassword' (Attached directly). A 'Permissions boundary' section indicates it is not set. A 'Generate policy based on CloudTrail events' button is present.

Step 8: In that permissions select Attach policies directly And select the policy which you want to Attach

The screenshot shows the 'Add permissions' step in the AWS IAM User Details page. The 'Attach policies directly' option is selected. A list of available policies is shown, with 'EC2Stop' selected. The 'Next Step' button is visible at the bottom right.

Step 9: Then click on Add permission on the tab

The screenshot shows the 'Add permissions' step in the AWS IAM console. The 'User details' section shows the user 'Tejaswi@23'. The 'Permissions summary' table contains one policy: 'EC2StartStopTerminate' (Customer managed). At the bottom right, there is a yellow 'Add permissions' button.

Step 10: So successfully we gave the permissions to the policy Now we can check as below steps

The screenshot shows the 'Permissions' tab for the user 'Tejaswi@23'. The 'Permissions policies' section lists three policies: 'AdministratorAccess' (AWS managed - job function), 'EC2StartStopTerminate' (Customer managed), and 'AmazonSSMPowerUser' (AWS managed). The 'Add permissions' button is located at the top right of the table.

Step 11: Now we have to login in to the user which we used above to give the permissions And then go to EC2 click on instances Then select the instance which you want to check. Here we successfully started the instance.

The screenshot shows the AWS EC2 Instances page. A green success message at the top left says "Successfully initiated starting of i-0946b61f9c56c8807, i-0fd308c9aff1ebebe". The main table lists two instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
MyFirstInstance	i-0fd308c9aff1ebebe	Running	t3.micro	3/3 checks passed	View alarms	eu-north-1b	ec2-16-170
MyFirstInstance	i-0946b61f9c56c8807	Running	t3.small	Initializing	View alarms	eu-north-1a	ec2-13-60+

Below the table, it says "2 instances selected". The "Monitoring" section is visible, showing CPU utilization, Network in, Network out, and Network packets in metrics over the last hour. The status bar at the bottom right shows the date as 03-03-2025 and the time as 12:13.

Step 12: Now we successfully stopped the running instance

The screenshot shows the AWS EC2 Instances page. A green success message at the top left says "Successfully initiated stopping of i-0946b61f9c56c8807, i-0fd308c9aff1ebebe". The main table lists two instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
MyFirstInstance	i-0fd308c9aff1ebebe	Stopped	t3.micro	3/3 checks passed	View alarms	eu-north-1b	-
MyFirstInstance	i-0946b61f9c56c8807	Stopped	t3.small	Initializing	View alarms	eu-north-1a	-

Below the table, it says "2 instances selected". The "Monitoring" section is visible, showing CPU utilization, Network in, Network out, and Network packets in metrics over the last hour. The status bar at the bottom right shows the date as 03-03-2025 and the time as 12:14.

Step 13: We tried to terminate the stopped instance but it showed an error. So, our Project is successfully Completed

The screenshot shows the AWS EC2 Instances page. On the left, a sidebar lists various EC2-related services: Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AHIs, and AH Catalog. The main content area displays a table titled "Instances (2/2) info". The table has columns: Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, Public IPv4 DNS, Public IPv4, and Elastic IP. Two instances are listed:

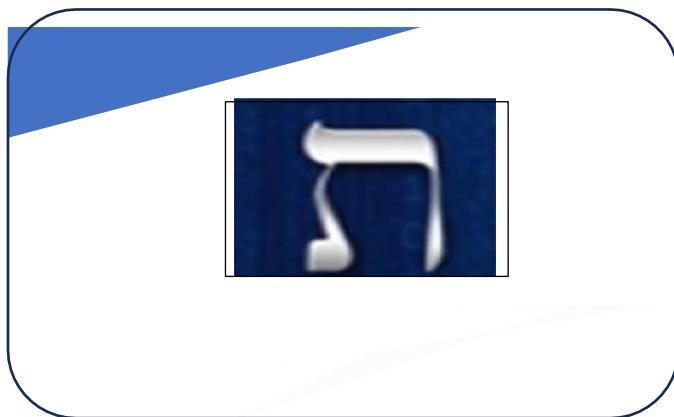
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4	Elastic IP
MyFirstInstance	i-0d30bc9aff1ebbe	Stopped	t3.micro	3/3 checks passed	View alarms	eu-north-1b	-	-	-
MyFirstInstance	i-0940b619c55c8807	Stopped	t3.small	Initializing	View alarms	eu-north-1a	-	-	-

A large red error message box is overlaid on the top right of the table, stating: "Failed to terminate [selected] an instance. You are not authorized to perform this operation. User: arn:aws:iam::997722670675:user/Sirang@123 is not authorized to perform: ec2:TerminateInstances on resource: arn:aws:ec2:eu-north-1:897722670675:instance/0940b619c55c8807 with an explicit deny in an identity-based policy. Enclosed authorization failure message: IAM-Swaggerify_IamNWhBfDUDr5E1DgjYw0tH3ggpH4tL_QzCQWB3dYTTP5jekHHTLjCg_bJmltY0dyhugB_wglmQoSBUSfhs-g2UyVZbX97Cleas38_XvCH77enpby0F9Y1XKKA0H4t9vG5ynB5-urmn5M47SQfElxTQqnfRbMs5dgVmst14900v9_4_H_P72BAMN7Xy2naeHd9g-KHhzt911_Vbd1uQS0L4uJ8cRcRORFRBvewC8Ml-yhLg7G9n4HOrXydoXgkxyT7U4t9puytpOTDpIwlyOJBly-8ke_11N087swqgV1QfQ_88WVtggA2_r0tqgUGx32fhePywQf2P7fhwG2VlnEdGNgspun3c2Ybym3peGv5wvkl05914PfToAc2CoP-wje-DNvmtDwRtf2Gm0lta1Mg-9K2zpd851135vPN40_S5g2odg-d7_2AQ9Y9ymNuvLUEfjPKL_BE3kQ_Q62h0nPrzA/m5a2f9p_59HMKmTrn5052_7AaQfR1Yc03tgAMP9jO62TfJsl.lhvDgftBWf5cgPOpfrw281mzjMVE95AV9lp3J8WVAM9OpwWfWso5uTu7ycn50Xjh240OoflwWOryx5PhlxWtLH8jtcAPewW99eQfRgTVHf-fc_GZTb6cwdu6y722mz14457L7LWf4PPfzyoDrmpCU8yfouE-cvN-m7el0995nrlw2Q00hQzfhd57EZD5m5yqf9sdRvYQkqnt-(p5130Pj1A9Ne6u802wv3s9p5Wk5ipQGeK_xuMT7mr2z9tLoCell6dellfWAheliTQf9p-JGtHfVw6l1vwnV99n8dUjcrUctRUQJ2vshPK5dJhkglopoQz2zdH2jAgRLU6eCUYQDriBw_SjH0_KODIfnX4PnP8



ADHOC NETWORK TECH, VIZAG

ADITYA DEGREE COLLEGE, RAMNAGAR(LONG TERM INTERNSHIP)



CREATE A FILE STORAGE IN DROPBOX

MINI PROJECT-2

TEAM MEMBERS

*T.Tejaswi
D.Tejaswini
K.chinmayi
M.sravanthi
K.vijaya joytha*

INTRODUCTION

In today's digital age, the need for secure and scalable file storage solutions has become more critical than ever. Cloud storage platforms like Dropbox have revolutionized the way individuals and businesses store, manage, and share files over the internet. Dropbox, a cloud storage service, allows users to store files, synchronize them across devices, and share them with others easily. This project aims to demonstrate how to create a robust file storage solution in Dropbox using Amazon Web Services (AWS) to automate and manage file uploads to Dropbox from within a cloud environment.

The integration of Dropbox with AWS enables users to leverage the power and scalability of cloud computing while providing an intuitive interface for file management. Using AWS services like Lambda, S3, and IAM (Identity and Access Management), we can automate the process of uploading files, synchronizing them with Dropbox, and setting permissions for access control. This project will implement a solution that will allow users to interact with Dropbox through the AWS environment, ensuring both flexibility and security.

This project not only helps in understanding Dropbox's API and its integration with AWS but also explores automation techniques that can greatly enhance productivity in business workflows. Furthermore, by using AWS services, this solution ensures scalability, security, and ease of access to the stored files across multiple devices and applications. The main objective of this project is to automate file storage operations, such as uploading files, synchronizing directories, and enabling real-time access to files in Dropbox, while utilizing AWS as the backbone for all automated processes.

Problem Statement

With the rise of remote work and digital collaboration, the need for a cloud-based file storage system that is both reliable and accessible is paramount. Dropbox has emerged as one of the most popular platforms for such purposes. However, manually managing files on Dropbox can be time-consuming and prone to errors. By automating file uploads to Dropbox using AWS, we can streamline this process, ensuring that files are uploaded consistently and securely. The integration should be able to handle file uploads from AWS S3, user authentication, and permission management for secure file sharing.

Objective

The objective of this project is to build a file storage solution within Dropbox, leveraging AWS services to automate file uploads and synchronize files across Dropbox. The project will focus on creating a secure, scalable, and easily accessible file storage solution by integrating Dropbox's API with AWS services.

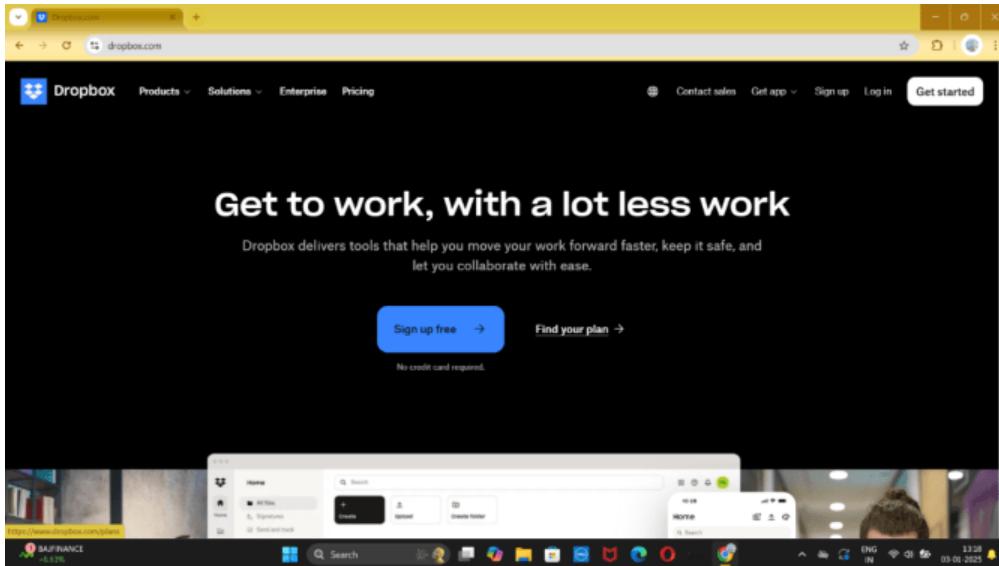
ALGORITHM

1. *Set Up Dropbox App:*
 - o *Create a Dropbox Developer account and set up a new app to get the API Key, App Secret, and Access Token.*
2. *Set Up AWS Services:*
 - o *Create an S3 Bucket: For storing files temporarily before uploading them to Dropbox.*
 - o *Create a Lambda Function: The function will trigger when a file is uploaded to S3 and handle uploading it to Dropbox.*
 - o *IAM Role: Assign the necessary permissions for Lambda to access the S3 bucket.*
3. *Create Lambda Function:*
 - o *Use the Dropbox API to authenticate and upload files to Dropbox.*
 - o *Trigger the Lambda function whenever a file is uploaded to the S3 bucket.*
4. *Lambda Code:*
 - o *Fetch the uploaded file from S3.*
 - o *Use the Dropbox API's files_upload method to upload the file to Dropbox.*
5. *Test the Process:*
 - o *Upload a file to S3 and verify that it is automatically uploaded to Dropbox by Lambda.*

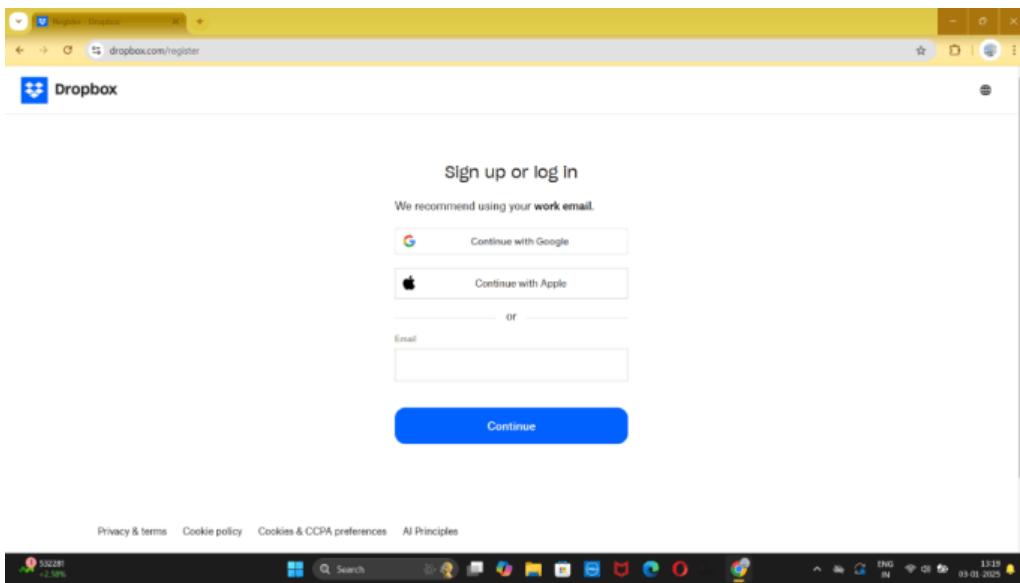
Dropbox

Objective: [CREATE A FILE STORAGE IN DROPBOX](#)

Step 1:- : Go to Google and type dropbox.com to open official drop box website

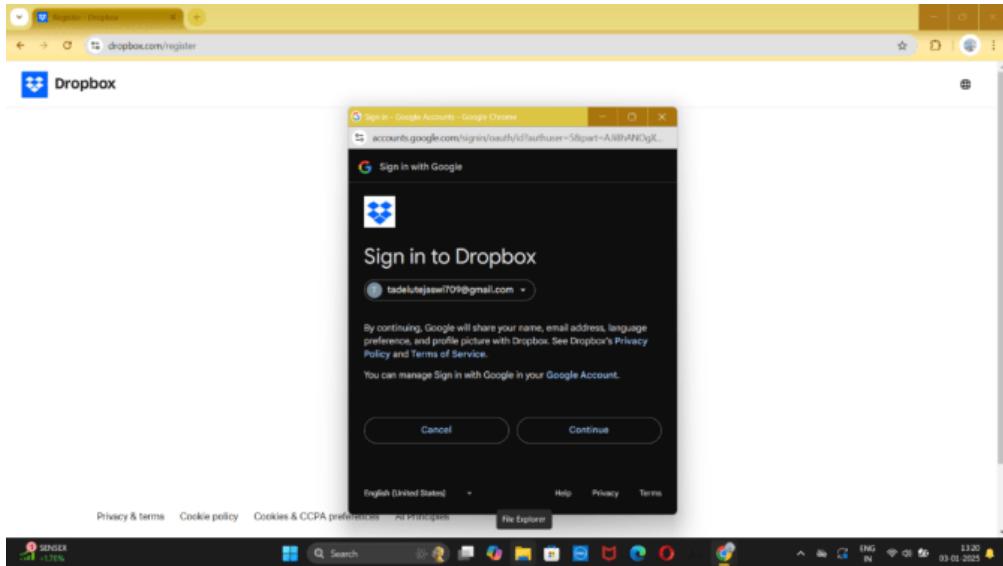


Step 2:- Choose sign up for free and enter your E-mail



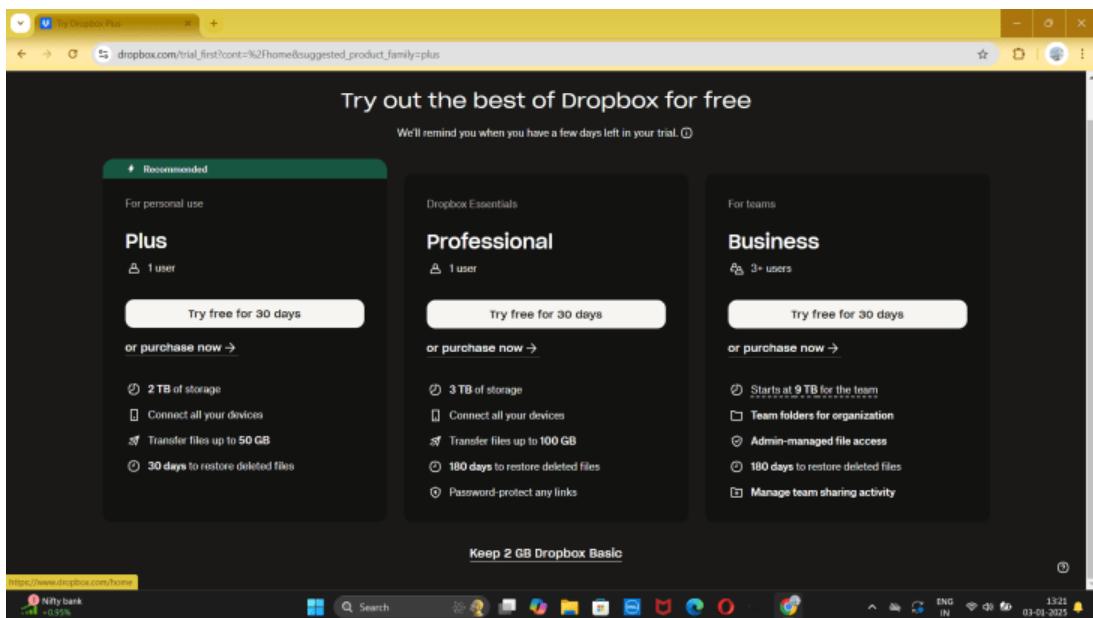
Step 3:-

Fill the details of the individual

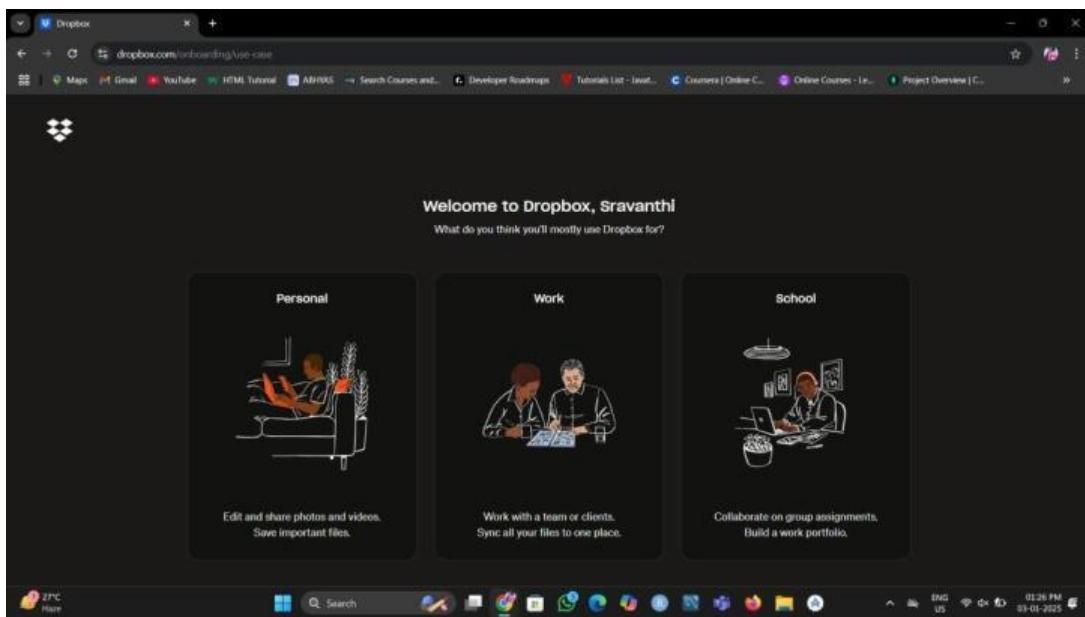


Step 4:-

Choose 2GB drop box basic

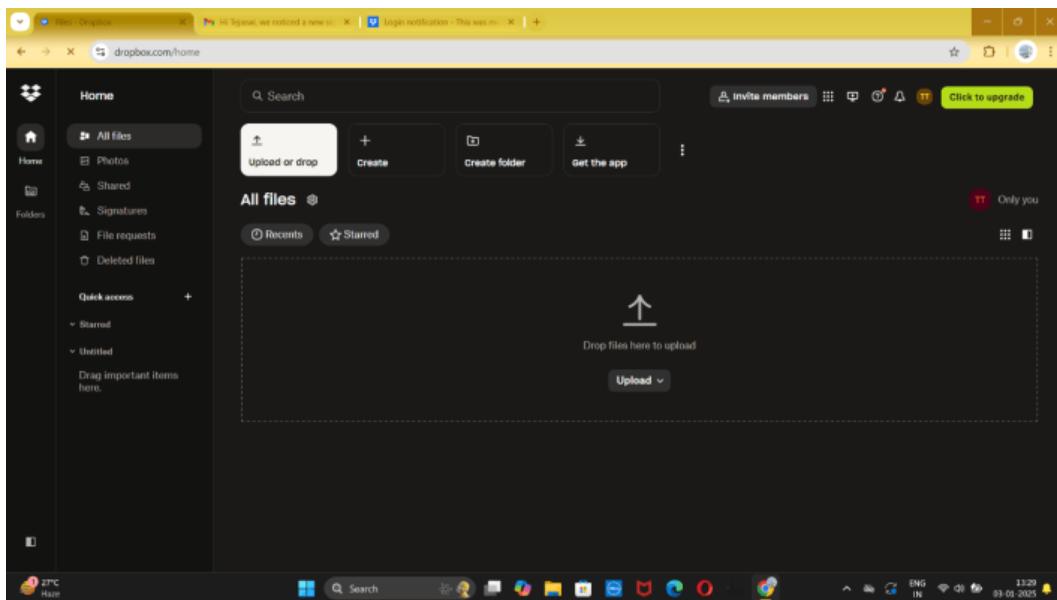


Step 5:- Select the option “Personal”

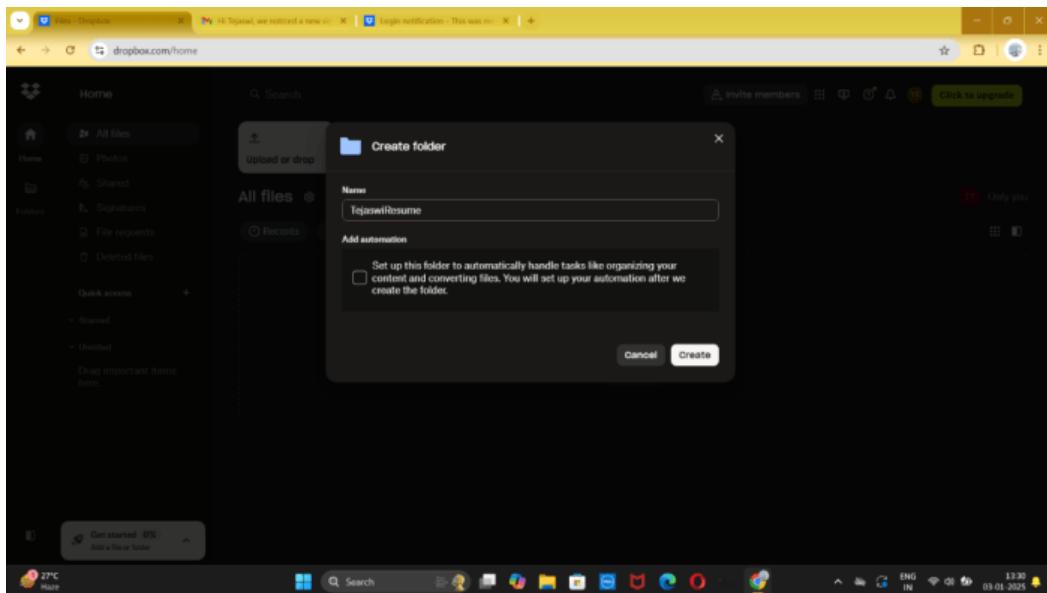


Step 6:-

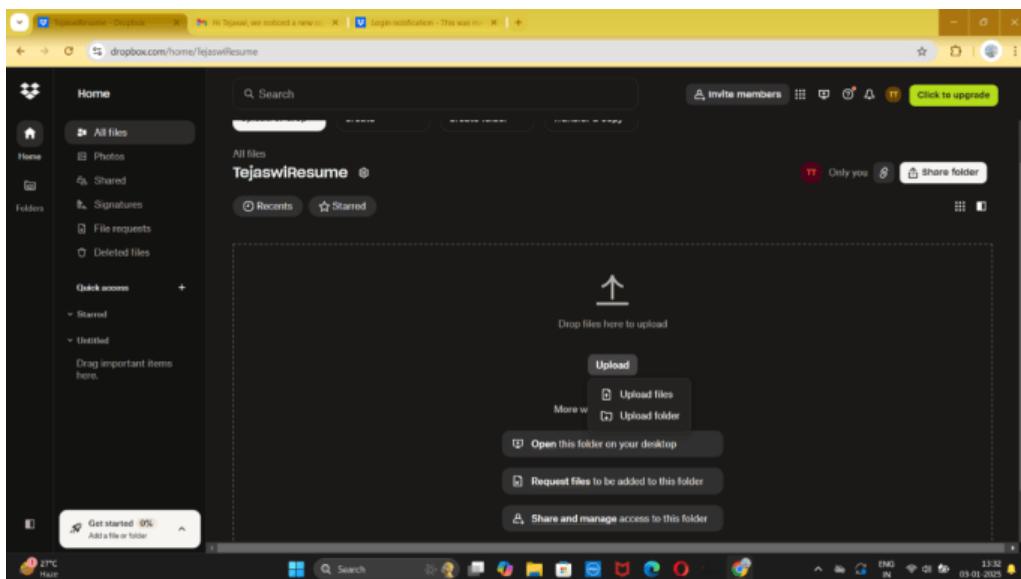
Home page will be opened



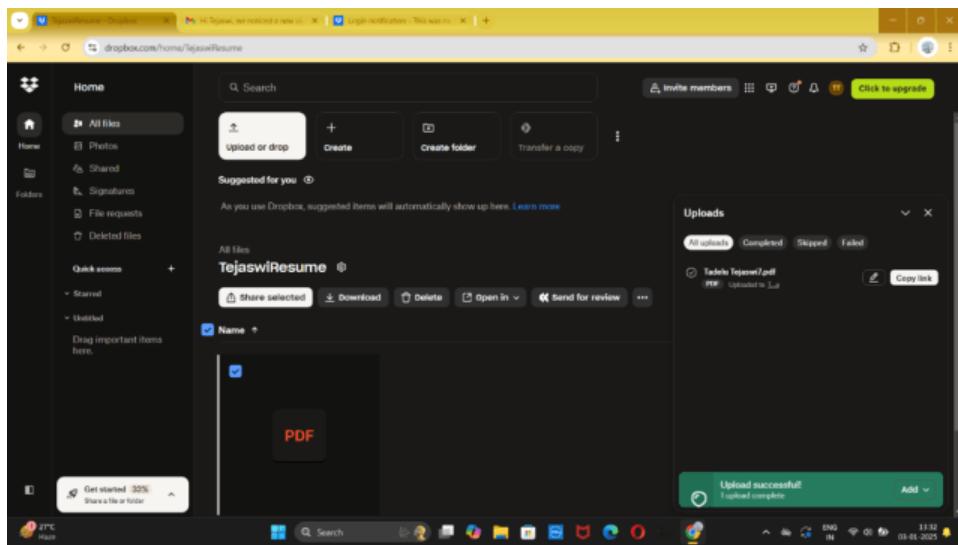
Step 7:-Create a folder



Step 8:-Upload the resume



Step 9:-Your resume will be uploaded successfully



MAJOR PROJECT



ADHOC NETWORK-TECH COMPANY, VIZAG

*ADITYA DEGREE COLLEGE, RAM NAGAR
LONG TERM INTERNSHIP*

**Host a static website using AWS S3
-- Major Project**

BY - T.TEJASWI

HOST A STATIC WEBSITE USING AWS S3

AGENDA

Title

Introduction

Algorithm

Process

Conclusion



HOST A STATIC WEBSITE USING AWS S3

INTRODUCTION:

To host a static website using AWS S3, you will leverage S3's object storage capabilities to store your website's HTML, CSS, and JavaScript files, and configure S3 to serve them directly to your users over the internet.

- What is S3?
 - Amazon S3 (Simple Storage Service) is a powerful, scalable object storage service within Amazon Web Services (AWS).
 - Static Website:
 - A website composed primarily of HTML, CSS, and JavaScript files, where content is not dynamically generated from a database.
 - Why S3?
 - S3 is an ideal choice for hosting static websites due to its durability, scalability, and cost-effectiveness.

CHARACTERISTIC

.Scalability and Durability:

- S3 is designed for high scalability and durability, ensuring your website is accessible even with fluctuating traffic and provides data protection with 99.99999999% durability.**

•Cost-Effectiveness:

- S3 offers a pay-as-you-go pricing model, so you only pay for the storage and data transfer you actually use.**

•Simplicity:

- The process of setting up website hosting is straightforward, primarily involving creating a bucket, enabling website hosting, and uploading your static files.**

•No Servers Required:

- You don't need to manage web servers or operating systems, reducing operational overhead**

ALGORITHM

Step 1:- Create an S3 Bucket

Step 2:-Configure Static Website Hosting

Step 3 :- Upload Your Website Files

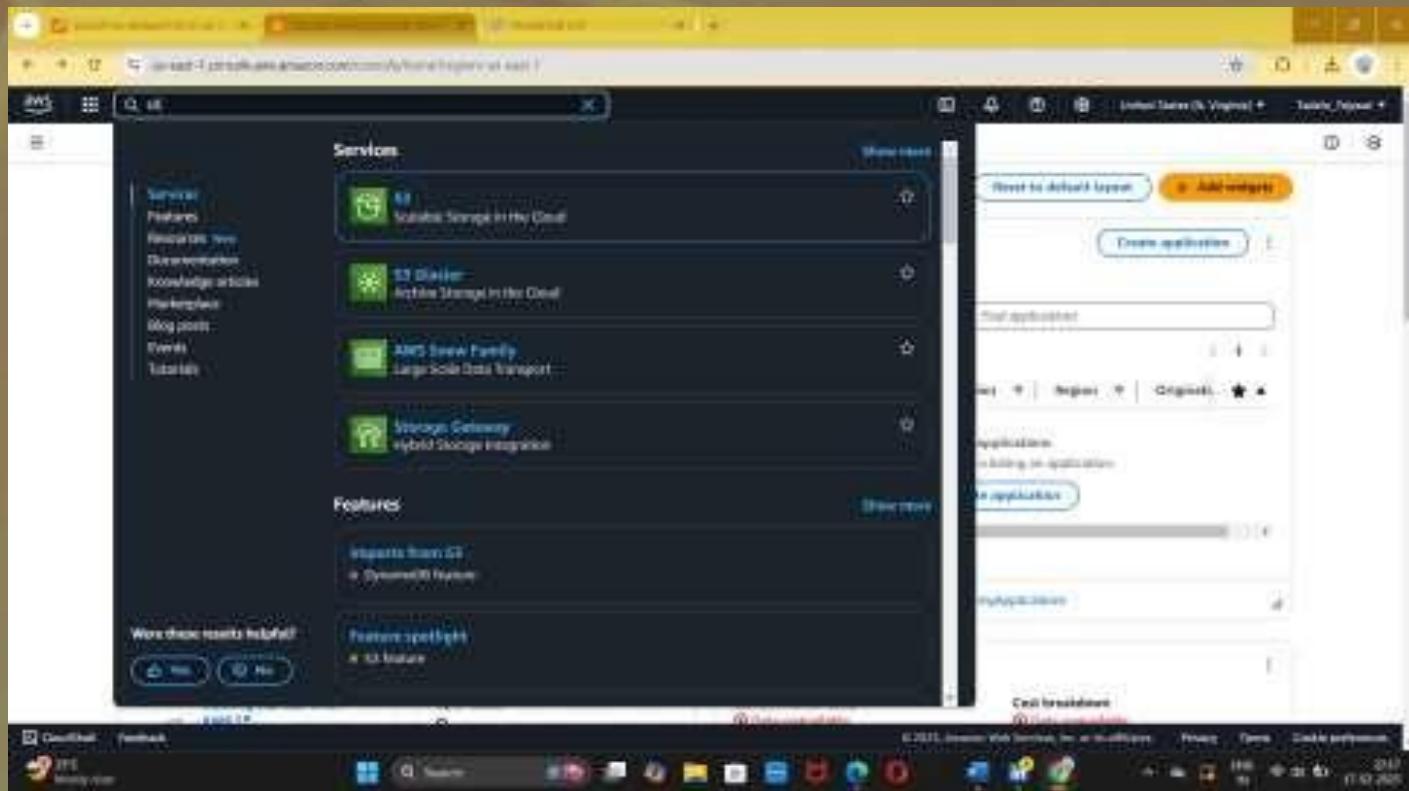
Step 4 :-Set Permissions for Public Access

Step 5:- Configure CloudFront for Distribution:

Step 6:- Connect a Custom Domain (using Route53)

MAJOR PROJECT

- Creating of S3 Buckets and Objects
Search S3 in the console home page



Click on create object

The screenshot shows the Amazon S3 service page. The main heading is "Amazon S3" with the subtext "Store and retrieve any amount of data from anywhere". A callout box on the right says "Create a bucket" and provides instructions: "Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored." Below this, there is a "How it works" section with a video thumbnail titled "Introduction to Amazon S3" and a "Pricing" section with information about no minimum fees and pricing based on location. At the bottom, there is a "Resources" section.

Define AWS Region and Bucket name

The screenshot shows the 'Create bucket' wizard on the AWS S3 service. The current step is 'General configuration'. It includes fields for 'AWS Region' (set to 'US East (VA) us-east-1'), 'Bucket type' (set to 'General purpose'), and 'Bucket name' (set to 'myawsbucket'). There are also sections for 'Copy settings from existing bucket' and 'Object Ownership'.

Have a look on default settings and click on create Bucket.

The screenshot shows the 'Create bucket' wizard on the AWS S3 service. The current step is 'Default encryption'. It includes options for 'Encryption type' (set to 'Server-side encryption with Amazon S3 managed keys (SSE-S3)'), 'Bucket KMS' (set to 'Disable'), and a link to 'Advanced settings'.

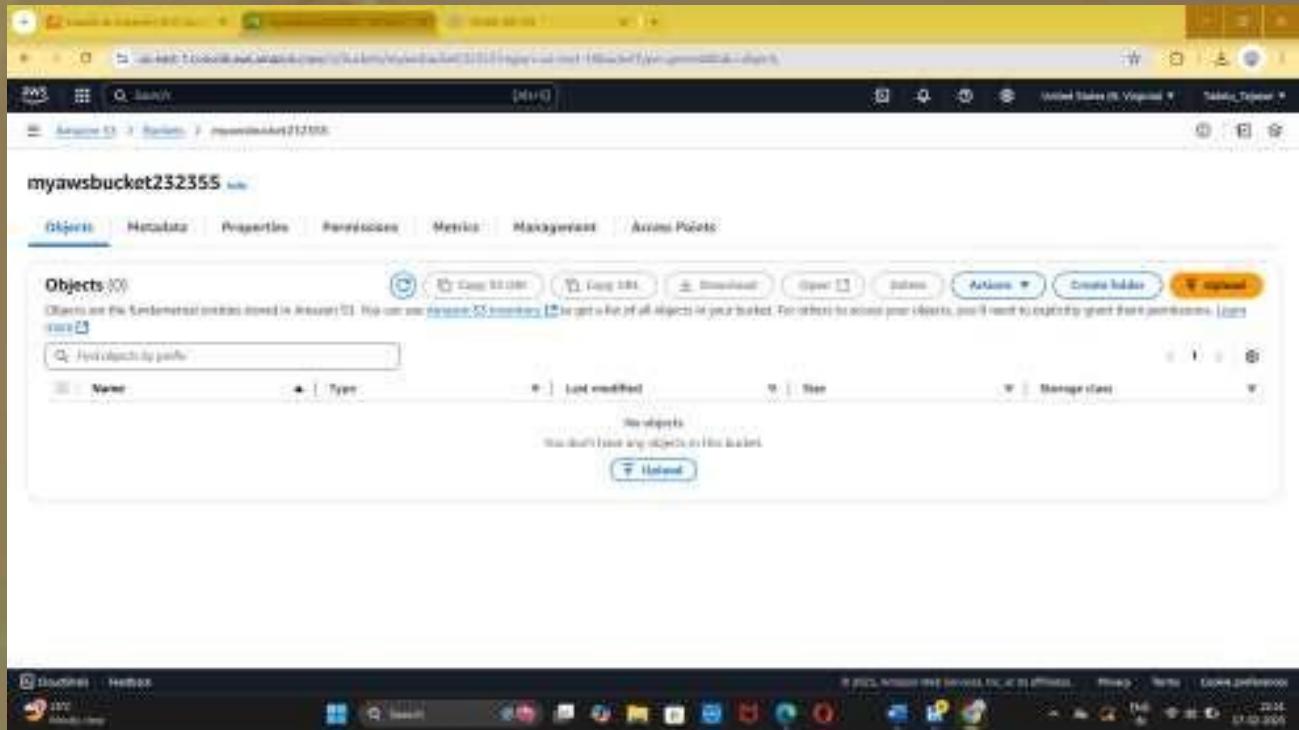
Successfully bucket will be created

The screenshot shows the AWS S3 console with a green success message at the top: "Successfully created bucket 'myawsbucket232355'". Below it, there's an "Account snapshot" section with a link to "View details". Under "General purpose buckets", a single bucket named "myawsbucket232355" is listed, showing its creation date as February 17, 2023.

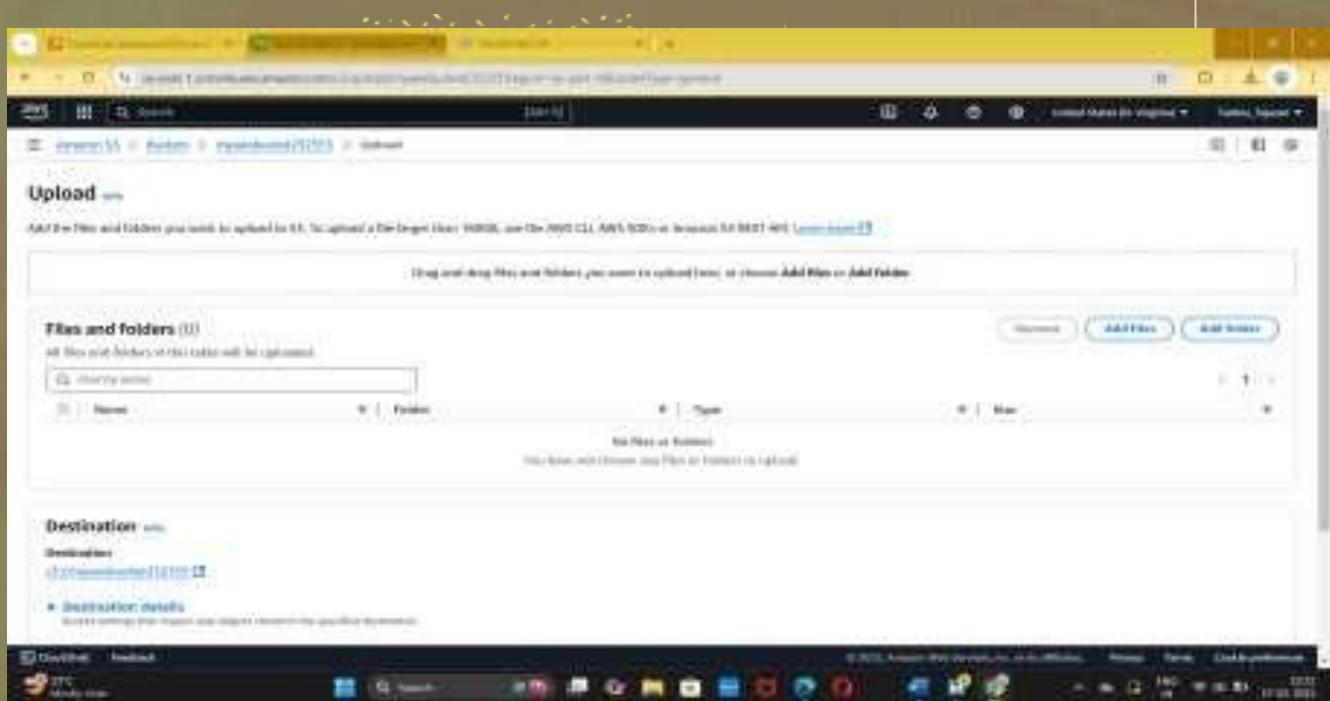
Click on your bucket

The screenshot shows the AWS S3 console with the newly created bucket "myawsbucket232355" selected. The "Objects" tab is active, showing a message: "No objects. You don't have any objects in this bucket." There are several action buttons at the top: "Upload", "Actions", "Create folder", and "Edit".

0 objects will be appeared



Click on upload. Click on upload object and click on upload



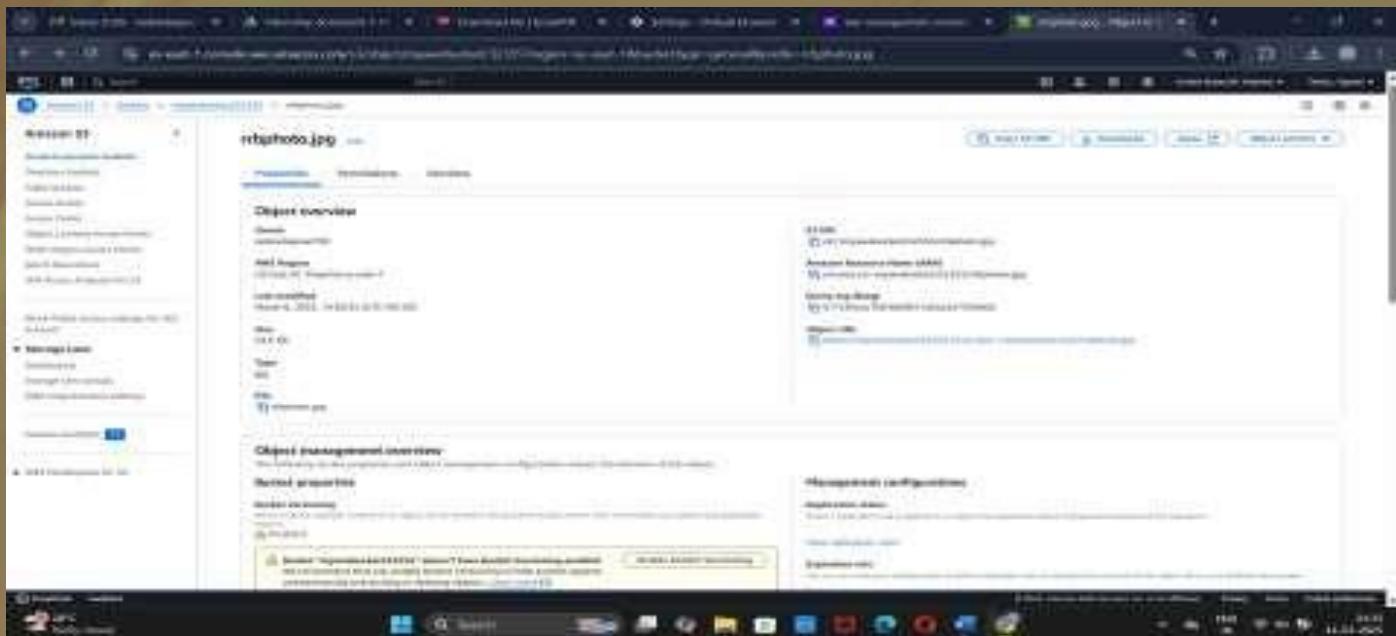
Successfully will be uploaded

The screenshot shows the AWS S3 console with a green success message at the top: "Upload succeeded! For more information, see the Files and folders table." Below this, a summary table shows one file uploaded successfully and one failed. Under "Files and folders", there is a table with one row containing a file named "apple.jpg". The file is 54.5 KB and was uploaded successfully. The browser's address bar shows the URL for the upload operation.

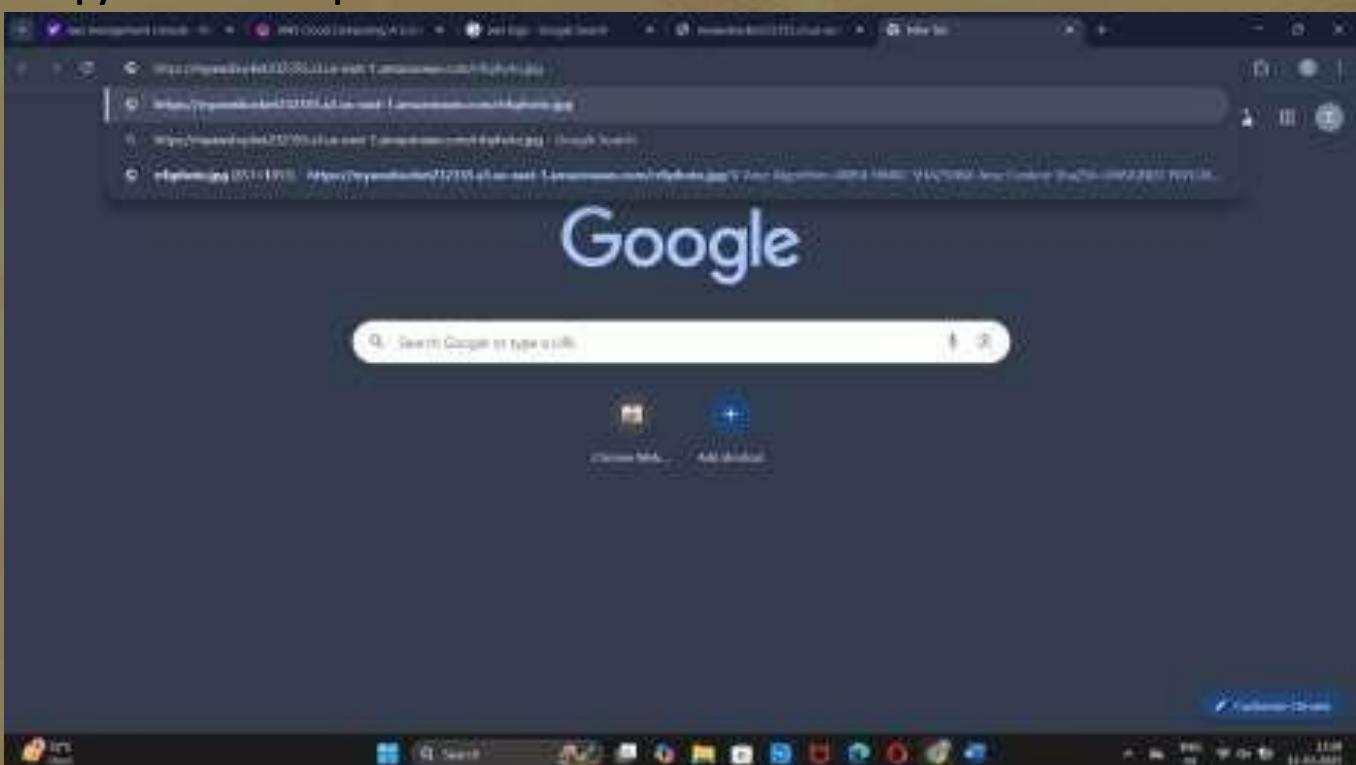
Go to objects and click on the object you have created

The screenshot shows the AWS S3 console with the "Objects" tab selected. It displays a list of files in the bucket "mynewbucket252355". One file, "apple.jpg", is visible in the list. The browser's address bar shows the URL for the objects page.

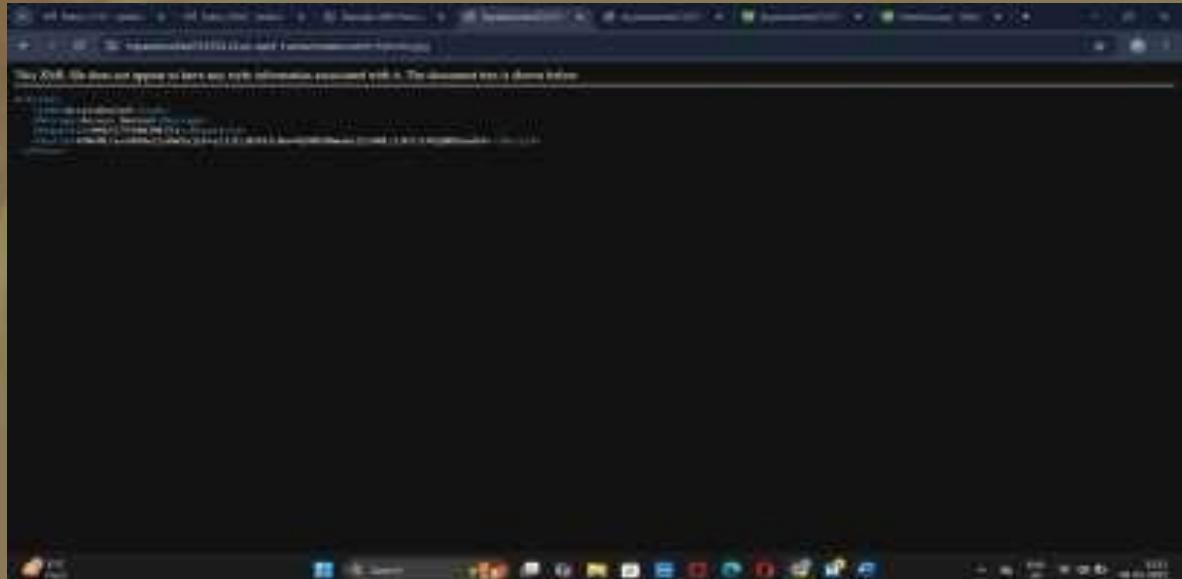
Object details will be overviewed and click on open



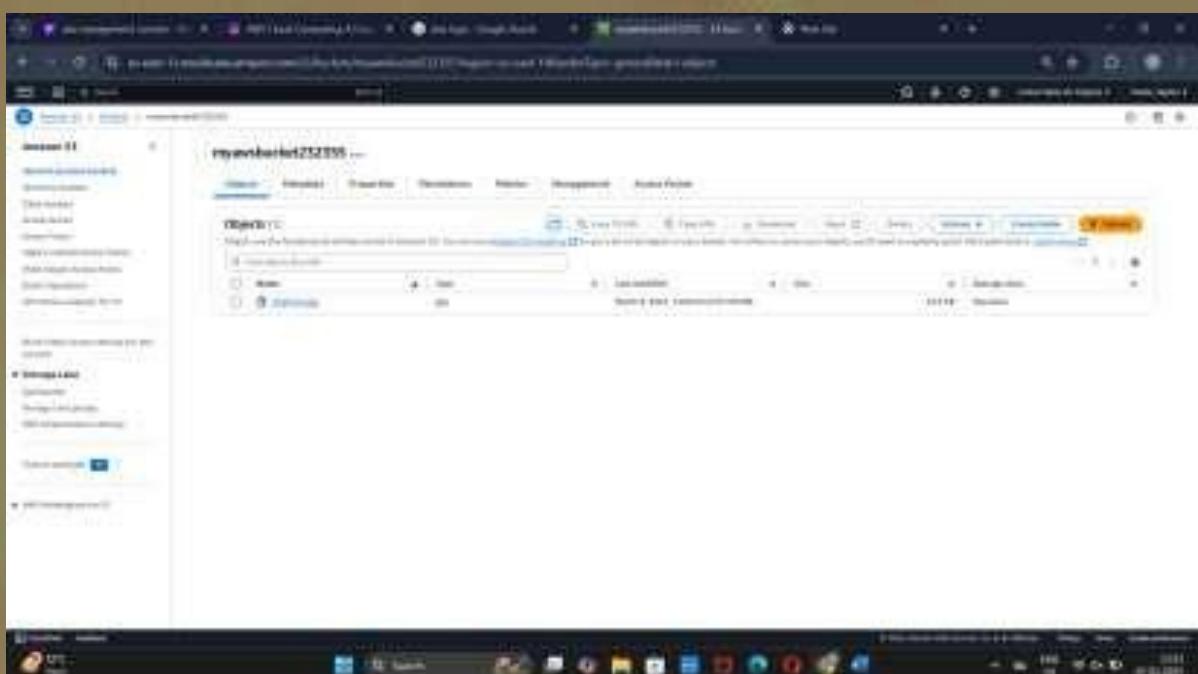
Copy the URL and open it



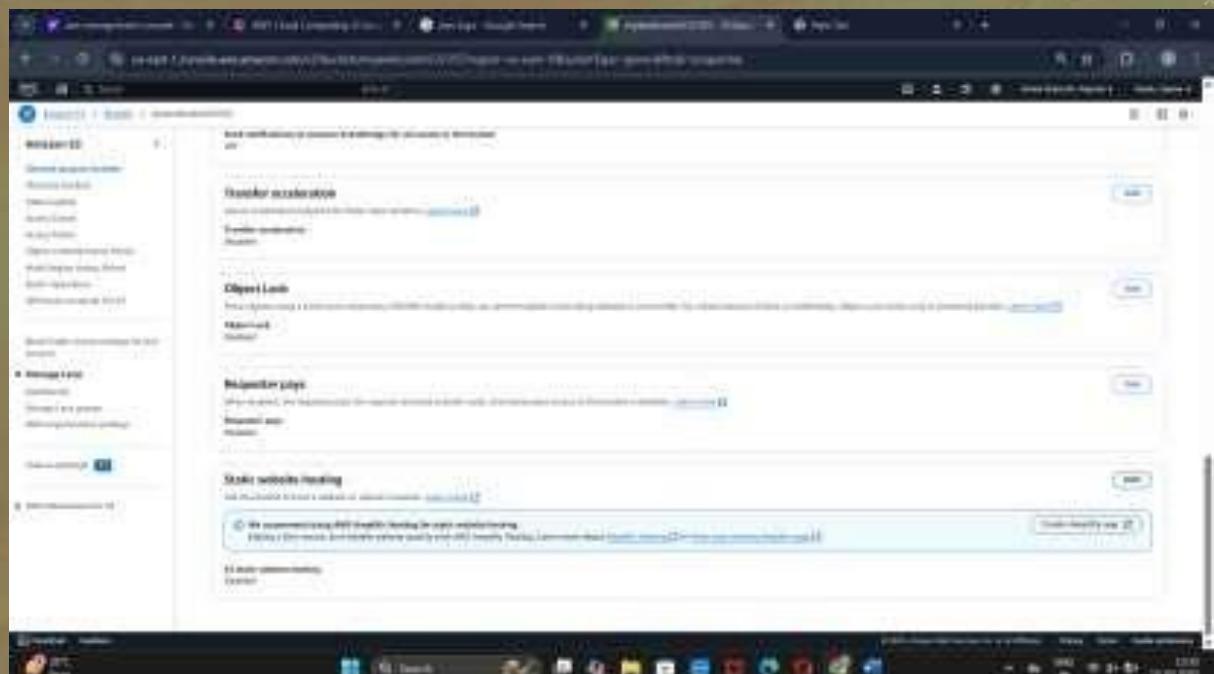
If you receive an error in this way you need to follow these procedures



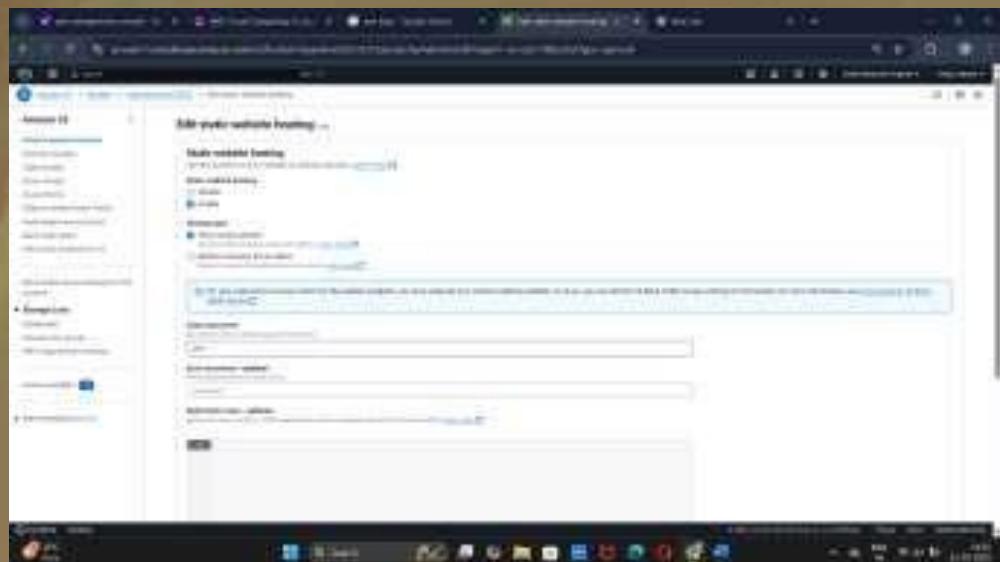
Click in properties to enable settings in public view in window



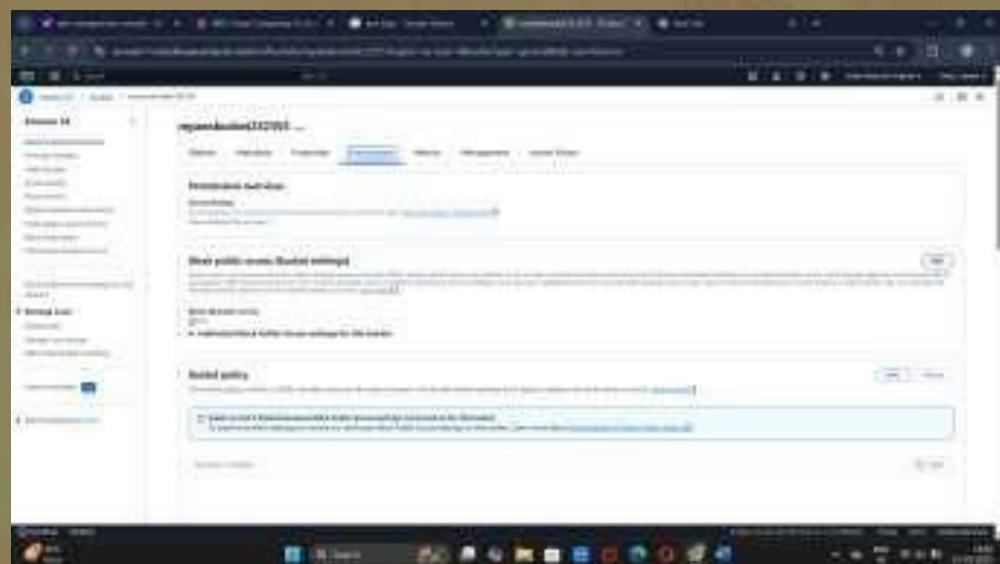
Click on edit in STATIC WEBSITE HOSTING



Click on Enable and hosting type and choose the options as below and enter index document name that you want to insert



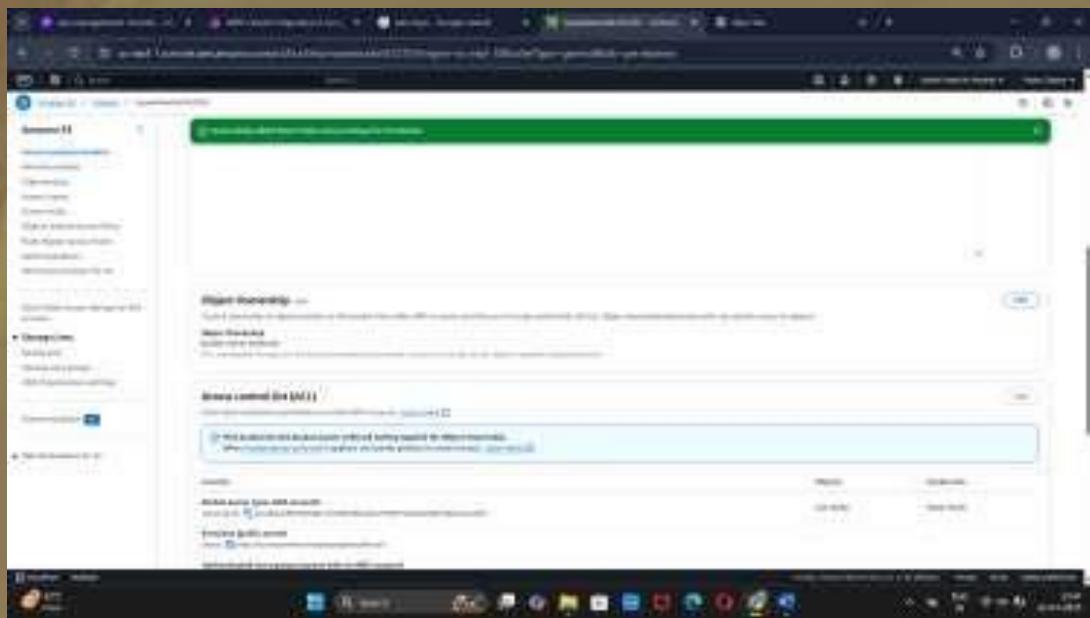
Now click on PERMISSIONS and select edit option in BLOCK PUBLIC ACCESS



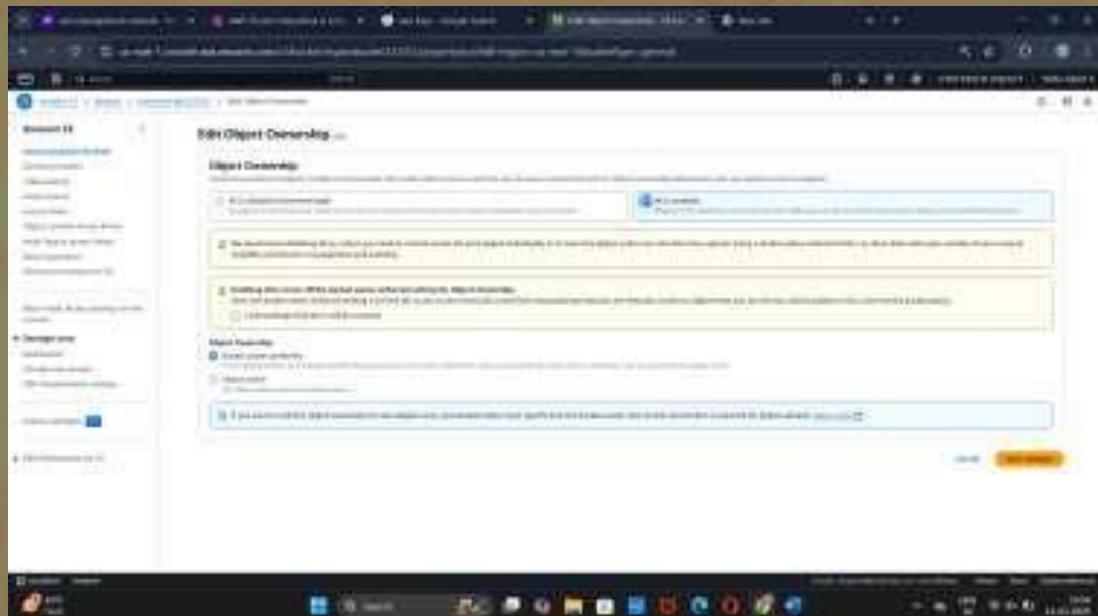
Remove the tick mark on the block all public access as shown and click on save changes



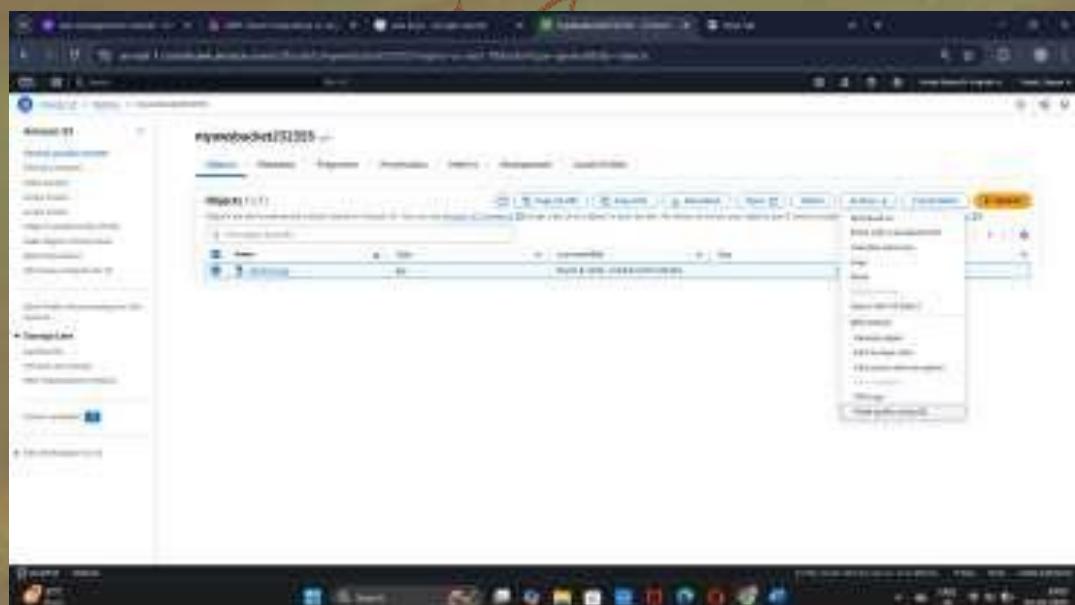
Again,in PERMISSIONS go to object ownership and click on edit



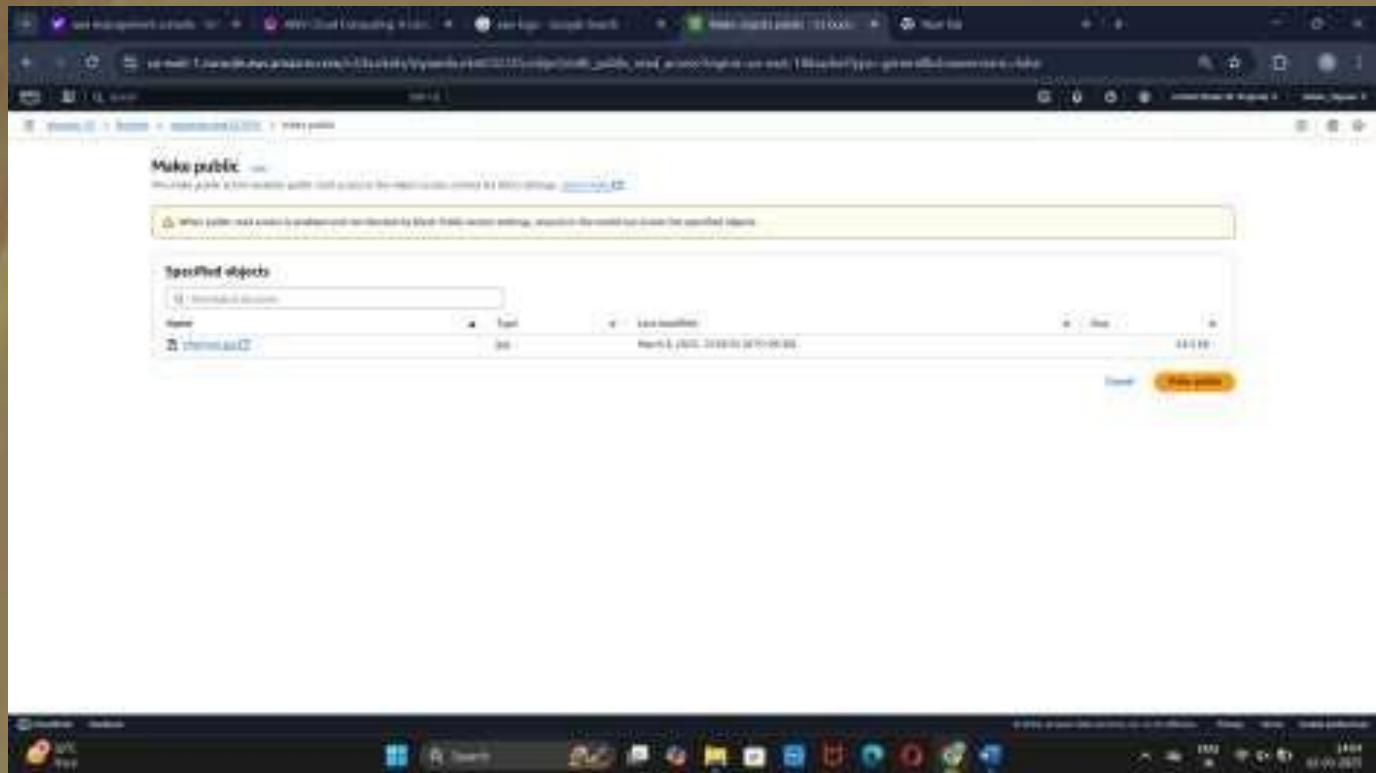
Click on ACL enabled and I acknowledge and save changes and confirm it



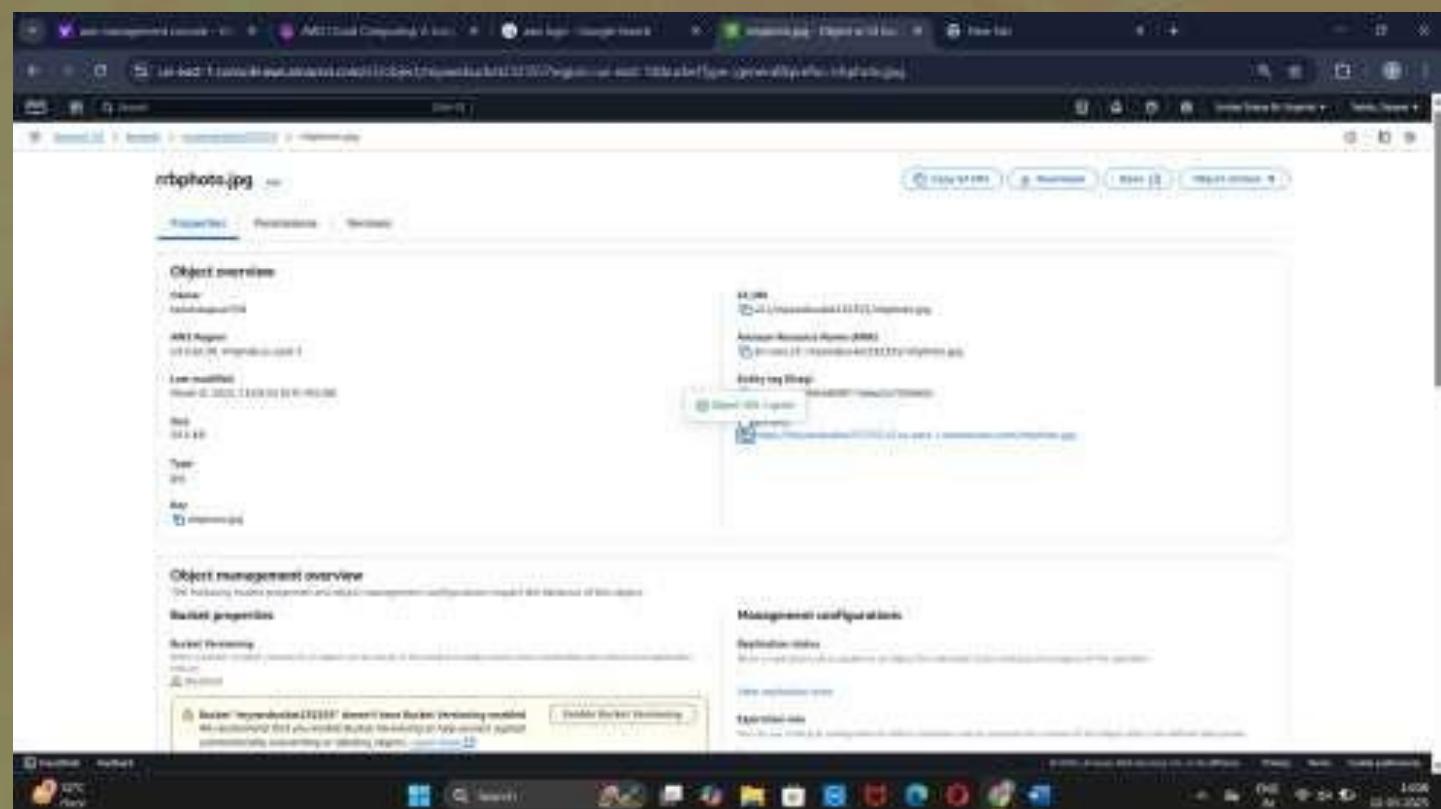
Again, go to objects and click on the actions to enable the changes to the bucket file
ACTION->MAKE PUBLIC USING ACL



Click on MAKE PUBLIC



Now click on the file and copy URL



Paste the URL in the new window



Now successfully the picture will be shown



CONCLUSION

Hosting a static website on AWS S3 provides a cost-effective and scalable solution for serving web content, allowing you to leverage the power of cloud computing for a reliable and performant web presence, according to multiple

- Cost-effective
 - You only pay for the storage and data transfer you use, rather than the cost of running and maintaining servers.
- Scalable:
 - Easily handle increased traffic and demand with S3's ability to scale on-demand.
- High Availability:
 - S3 is designed to provide high availability and durability, ensuring your website remains accessible even if infrastructure issues occur.

THANK YOU