**Authentication flow using AWS services**

* AWS Cognito provides an authentication service for applications and its serverless. We don’t need to manage any database or servers to handle user data and authentication flows, we can leverage Cognito to handle those tasks.
* A simple way of doing this would be to include a secret key of an AWS user to enable access to AWS resources. But this is less secure and it’s not possible to restrict access to certain users. That’s where user authentication comes in to play either with AWS Cognito or with external authentication providers.
* To allow AWS resource access to users with authentication providers in Cognito, “Identity Pools” are used. Identity pools can provide AWS Access via multiple external authentication providers such as Facebook, Amazon, Google, OpenID connect providers and SAML Identity providers. This is called federated authentication.
* To successfully authenticate a user, AWS Cognito needs an Identity pool and a token received from an external authentication provider or from AWS Cognito authentication provider itself.
* Using an external provider is comparatively easy because the provider handles the user sign up, sign in and password management for us.
* AWS Cognito provides the ability for us to configure our own identity (Authentication) provider. Which means the control of the user sign up, sign in, password management and many more user management features are in our hands.

Main steps of this process are as follows in order --

* **User Registration**  
  User enters email, username and password and registers with the User Pool.
* **User Verification**AWS Cognito User Pool will send verification code by email or SMS and the user enters the code to get verified with the User Pool.
* **User Login**User enters username and password and logs in with Cognito User Pool in which case a token will be provided by Cognito upon successful login.
* **Get Temporary Credentials**Cognito Identity Pool will provide temporary credentials to AWS resources using the token that was received on successful login.
* **User Authorization**Cognito will authorize the user with necessary permissions with IAM role.
* **AWS Resource Management**Authorized user can manage AWS resources according to the permissions given by AWS IAM.  
    
  A picture containing chart

  Description automatically generated

**Workflow**