Authentication and Authorization:- Authentication check who are you.. by checking the user credentials from authentication servers whereas authorization checks what permissions of access to a particular service do you have .

OAuth:-

OAuth is an open authorization protocol that allows a service to gain limited access to another service on behalf of a user so it is meant for a service to authorize another service with limited Access provided by the user for example if we want to print photos on a site without actually downloading it from our google drive we would not give our google id and password to another service as we cannot trust other service provider so we would want the service to only use our photo from our drive without giving access to our account so here OAuth is use so that we would only give some limited access to other service to access only those part which we want to give access so what OAuth would do is it will generate a token containing the list of services that we want to give access to a third party that token is used by other service to access only those service that it can access by using the token. Nowadays we use only OAuth 2.0 as OAuth 1.0 was very complex & not so scalable.

Just like in Github we can share our repo. Having public access so that the intended user can only read the code but cannot edit our code.

The main components of OAuth are:-

1. Actors:- The main actors that plays role in a OAuth are Resources which is protected data that require OAuth to access them. Then Resource owner which owns the data in the resource server like a user Google Drive account , resource server the API which stores the data like Google photos and the Client which is the third party application that wants to access our data.
2. Scopes and Consent:- The scopes defines the specific actions that apps can perform on behalf of the user. They are the permissions asked by the client while requesting a token. For ex. If we have a token of github public repo. With read only token then we cannot edit in the code.

Working Flow:- Firstly the client requests authorization from authorization server . The authorization server authenticates the resource owner and informs the user about the client and the data requested by the client. After granting permission to access the protected data, the authorization server redirects the user to the client with the temporary authorization code. The authorization server authenticates the client , verifies the code then issue a token to the client after which the client can access the protected resources.