What is Authentication

Authentication is the process of identifying users and validating who they claim to be. One of the most common and apparent factors to authenticate identity is a password. If the user name matches the password credential, the essence is valid, and the system grants access to the user.

Interestingly, with enterprises going passwordless, many use modern authentication techniques like one-time passcodes (OTP) via SMS, or email, single sign-on (SSO), multi-factor authentication (MFA) and biometrics, etc. authenticate users and deploy security beyond what passwords usually provide.

What is Authorization

Authorization happens after a user's identity has been successfully authenticated. It is about offering full or partial access rights to resources like databases, funds, and other critical information to get the job done.

For example, in an organization, after an employee is verified and confirmed via ID and password authentication, the next step would be defining what resources the employee would have access to.

Difference between Authentication and Authorization

Let's understand the core of utilizing authentication and authorization and how one differentiates from the other.

For instance, an organization will allow all its employees to access their workplace systems (that's authentication). But then, not everyone will have the right to access its gated data and resources (that's authorization).

Implementing authentication with the proper authorization techniques through a CIAM (consumer identity and access management) solution can protect organizations, while streamlined access will enable its workforce to be more productive.

A CIAM solution uses authentication and authorization technologies like JWT, SAML, OpenID Authorization, and OAuth.

Different Ways of User Authentication

- **Password-based Authentication:** It is a simple method of authentication that requires a password to verify the user's identity.
- **Passwordless Authentication:** In this method, a user is verified through OTP or a magic link delivered to the registered email or phone number.
- **2FA/MFA (Multi-factor Authentication):** It requires more than one security level, like an additional PIN or security question, to identify a user and grant access to a system.
- **Single sign-on (SSO):** It allows users to access multiple applications with a single set of credentials.
- **Social Authentication:** It verifies and authenticates users with existing credentials from social networking platforms.

Different Ways of User Authorization

- **Role-based Access Controls (RBAC):** It can be implemented for system-to-system and user-to-system privilege management.

- **JSON web token (JWT):** It is an open standard for securely transmitting data between parties, and users are authorized using a public/private key pair.
- **SAML:** It is a standard Single Sign-On format (SSO) where authentication information is exchanged through XML documents that are digitally signed.
- **OpenID Authorization:** It verifies user identity based on an authorization server's authentication.
- **OAuth:** It allows the API to authenticate and access the requested system or resource.

Database Design

Authentication And Authorization System

Find all Entities for the authentication and authorization system . first of find the basic entities (e.g User) and .
Learn details about the JSON Web token based Authentication and authorization?
Start Database design
Select and Database (learn about basic database mongodb and mysql)
Select and technology for the api or application will be done MVC Architecture
Or RestApi Based and decided the Frontend Technology