UserOperations:

Authentication Flow

1. Frontend (React or mobile)

- User enters phone number.

- Firebase sends OTP and verifies it.

- On successful OTP verification, Firebase returns an ID token (Firebase's JWT).

- This token is sent to your backend via Authorization header

2. Backend (Node.js / Express)

- Receives the Firebase ID token.

- Uses firebase-admin to verify the token.

- Gets user info (e.g., phone number, UID).

- Checks in your database:

- If user exists -> retrieve.

- If not -> create new user record using the verified phone number.

- Generates a custom JWT token (your app's JWT).

- Sends this JWT back to the client.

- JWT is used for all further authenticated API requests.

Why This is the Correct Way

Why This is the Correct Way:

- Firebase handles OTP verification securely and efficiently.

- Firebase ID token is short-lived (~1hr), minimizing misuse.

- Backend verification ensures token authenticity.

- Your custom JWT allows backend control over authentication.

- Database ensures persistent user identity.

- JWT used for stateless, secure API access.

User Registrations

=> create new user by using phone number

1. Login