SUPERVISOR: AHMED HANIF

NARWAL AUTH API DELIVERABLE 5

MUHAMMAD NASEEM
SAMI NAEEM
KYNAT MANSHA

Architecture Diagram

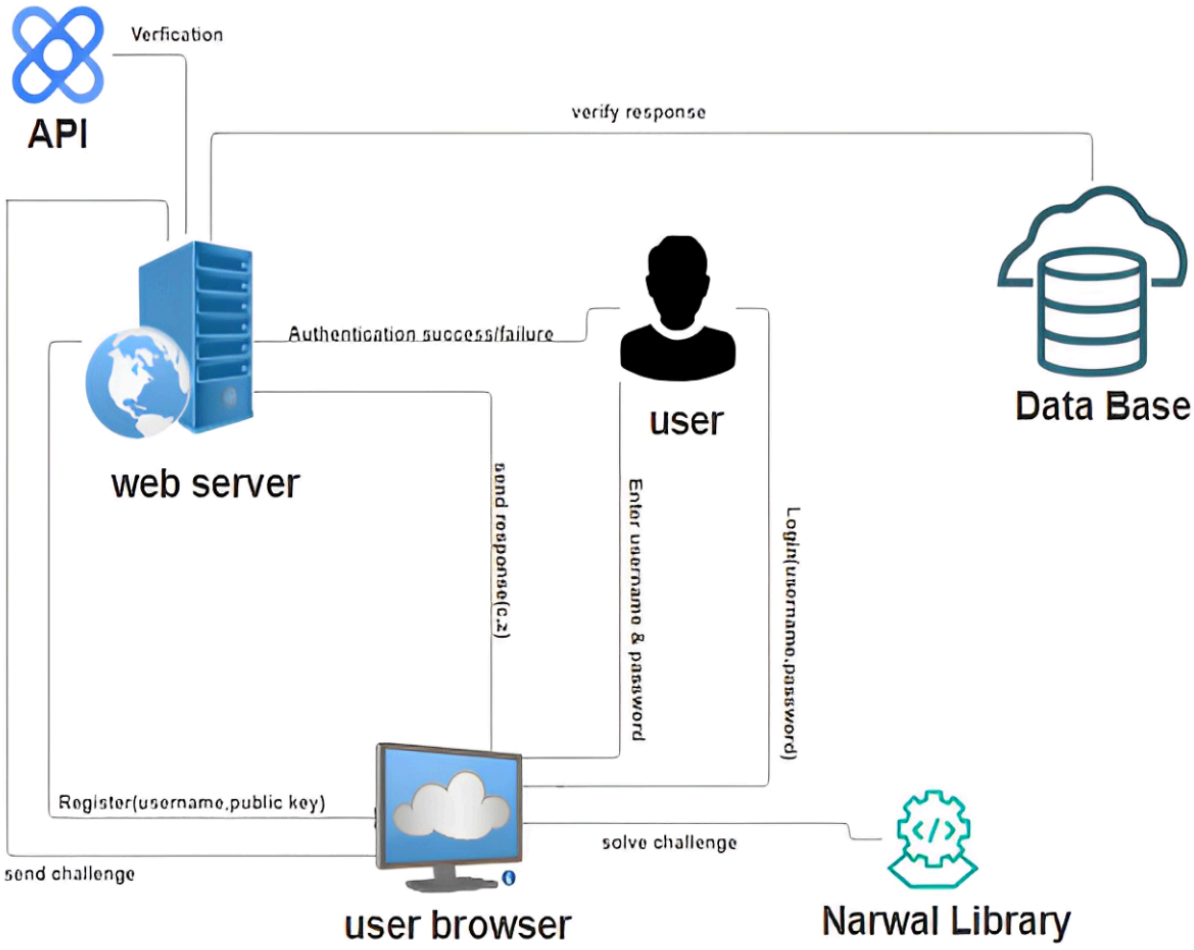

Diagram elaboration

Registration Phase:

- **User Registration:**
  - The user registers on the web server by providing a username and a public key.
  - The web server stores this registration information.

Login Phase:

- **User Inputs Credentials:**
  - The user enters their username and password into the user browser.
- **Challenge Generation:**
  - The web server sends a challenge to the user browser.

- **Challenge Response:**
  - The user browser, with the help of the Narwal Library, solves the challenge using the user's private key or other cryptographic means and sends the response back to the web server.

- **Verification:**
  - The web server verifies the response against the data stored in the database (which likely includes the public key associated with the username).

- **Authentication Result:**
  - If the verification is successful, the web server sends an authentication success message to the user.
  - If the verification fails, the web server sends an authentication failure message to the user.

Data Flow:

- **User to Web Server:**
  - The user sends login credentials (username and private key) to the web server.

- **Web Server to Database:**
  - The web server queries the database to verify the user’s credentials and the response to the challenge.

- **Web Server to User:**

- The web server informs the user about the authentication result (success or failure).

Role of Narwal Library:

- The Narwal Library plays a crucial role in solving the cryptographic challenge during the login phase. It contains functions and methods to handle cryptographic operations necessary for user authentication.

Description:
Our diagram illustrates the different components involved in the authentication process and their interactions. At the center, we have the user browser, which serves as the client-side interface for users to interact with our application.

The user browser communicates with the web server component, which is the central server handling incoming requests and authentication processes. When a user registers by entering their username and password, the client obtains the server's public key and performs the necessary computations to derive the user's public key Y, as per the protocol I explained earlier. The pair (username, Y, s) is then sent to the web server.

During the authentication process, the web server generates and sends a challenge in the form of a random number 'a' to the user browser. The user browser then solves this challenge by performing the required cryptographic calculations, with the help of our Narwal Library component. This library contains the necessary cryptographic functions and algorithms to facilitate the authentication protocol.

The solved challenge, represented as the pair (c, z), is sent back to the web server for verification. The web server verifies the response by computing T' and comparing the hash value with the provided 'c' value. If the verification is successful, the authentication is deemed successful; otherwise, it fails.

The user icon in the diagram represents an individual user interacting with the system through the user browser.

Additionally, we have the Database component, which stores user data and application data necessary for the authentication process and other application functionalities.

Our team has carefully designed this architecture to ensure a secure and robust authentication system, leveraging cryptographic techniques and the discrete logarithm problem to protect user passwords while enabling secure authentication. The Narwal Library plays a crucial role in facilitating the required cryptographic operations on the client-side, while the web server handles the server-side authentication processes and verifications.

Sequence Diagram