User Authorization Primer

Now that we have completely authenticated our user, it is now possible to implement authorization.

WE'LL COVER THE FOLLOWING

What is User Authorization?

Authorization is a security mechanism used to determine user/client privileges or access levels related to system resources, including computer programs, files, services, data, and application features. Authorization is normally preceded by authentication for user identity verification.

Types of Authorization

user-based

User-based authorization allows users to create, read, update, or delete their own data.

role-based

Role-based authorization occurs when you set up levels of access for different users. For example, an admin role might be able to access or delete anyone's information. A manager of a department store might have a role that allows him or her to see only their sales, refunds or other types of information that

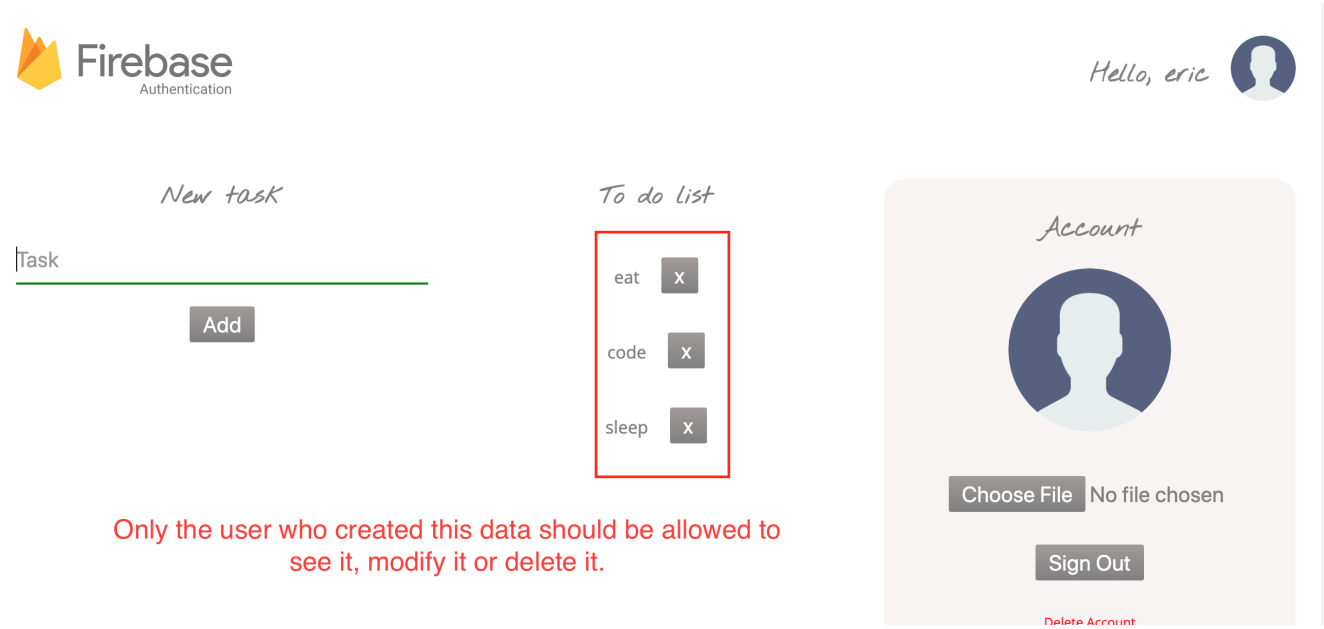
are appropriate for that *role* to see.

Building the To-Do List Application

For our application, we will use *Firestore Security rules* to provide access control. This allows us to build **user-based** access systems that keep our users' data safe. This course focuses on **user-based** authorization because it's the easiest to implement.

User-based Security in To-do List

This type of authorization allows a user to be able to read, write or delete items from lists that were created by them. They would not be **authorized** to read, write or delete items from any list created by someone else.



Taking Your First Step in *user-based* Security

Ready to protect your app against hackers? The first step is to add items to the database but also specify which user added them. We will do that in the next lesson!