Cors policy and how to stored cookie in backend ?

If we want to set cookie in the server side then we must follow the following steps

1st, in the client side in the app.js make sure axios.defaults.withCredentials=true ,

axios.defaults.baseURL = "https://airbnbhotels.up.railway.app"

axios.defaults.withCredentials=true

2nd , in the server side make sure the cors origin is the specific client url and

credentials:true

app.use(cors({

    origin: "https://airbnb-hotel-management-app.netlify.app",

    // origin: "http://localhost:3000",

    credentials:true

}))

3rd , if we want to store cookie in the client side from the server then we cannot make it happen and it will be very risky and security issue. So we store token in the server side so that no one can access the token easily and it is very much safety

How we can make it happen:

  res.cookie("token", token,{secure:true,sameSite:"none", }).json(user)

here to store the cookie in the server side we must declare the cookie to be

secure: true

samesite:none

if we can do that then we can store the cookie in the server side otherwise it will give error