How can I make my Online Book Library secure?

1. Which level of authentication is required for this application to be secure and ethical?
2. Which authentication methods are available and what are their advantages and disadvantages?
3. Which authentication method works better for this type of applications?
4. How to apply the research findings in my project
5. Conclusion
6. Sources

The “What” of this research is application for Online Book Library, where people can buy and read books and documents in written form. This type of application is widely spread in 21st century with the digitalisation of books.

The ”Why” is because I wanted to emphasize the security aspects of such applications and to take a look on what is considered ethical, regarding data collection, privacy and user transparency.

The “How” is achieved by using the DOT Framework. By using the Solidify method, which covers the “Field”, “Workshop“ and “Library” scopes, I can:

* Understand the user (Field) by personal observation, being one, survey and by exploration of user requirements
* Seek variation and improvement (Workshop) by brainstorming, prototyping, requirements prioritization and business case exploration
* See what guidelines and theories exist (Library) by design pattern researching, exploring best good and bad practices and doing a product analysis

1. Which level of authentication is required for this application to be secure and ethical?

To ensure the security and ethicality of an Online Book Library application, it is important to implement a tiered authentication system. It is crucial to adopt a model that includes least two levels of authentication, but at the same time we have to consider the ethical aspect of it.

One part of being ethical is to collect only the necessary information from the user to be able to use the application. In that case details like full name, email, password, date of birth and a consent to the Terms and Conditions are enough to be able to access the online store and eventually details of payment method. In most cases the details of the payment method are managed by a third-party software, but if not, this is also one very important aspect of the security.

Furthermore, the user has to be in control over their data and the application's features, over the privacy settings, to be able to opt-out of certain functionalities, and easily delete their accounts or data. This is called **User Empowerment**, which is part of **Compliance with Regulations in EU** called **“General Data Protection Regulation (GDPR)”.**

It's important rule when processing the personal data of EU residents to adhere to the GDPR's requirements.

Let’s not forget **Inclusivity - the inclusiveness and accessibility** to a diverse user base. Discriminatory practices must be avoided, and it must be ensured that the application caters to users with varying abilities, languages, and cultural backgrounds.

And finally, even if everything is legally implicated and documented somewhere deep in the terms and conditions for using the application, let’s not forget the moral obligation of being transparent with the customer about every action and update, regarding their data and privacy.

1. Which authentication methods are available and what are their advantages and disadvantages?

There are numerous authentication methods including:

* Biometric authentication: Uses unique biological traits for user identification (most of the times a fingerprint of face recognition). The advantages are that it includes high security and user convenience, but it may have privacy concerns.
* Password authentication: Traditional and effective, it relies on a combination of username and password. Advantages include simplicity, but a weakness may be a potential breach leak, due to weak passwords or user negligence.
* Two-factor authentication (2FA): Adds an extra layer of security, typically involving a secondary one-time code sent to a registered device. Enhances security, but user experience may be slightly more complex.
* Single Sign-On (SSO): Allows the user to access multiple services with a single set of credentials. Enhances user experience but may pose a security risk if the credentials are compromised.

1. Which authentication method works better for this type of applications?

In the case of Online Book Library, the methods of having a password with an additional optional layer of protection of 2FA are considered enough to protect the user data in most cases.

Everything above that like the Biometric authentication shouldn’t be mandatory for the purpose of this application. It could be, for example a fundamental part of an online banking application, where the user has to authorize important access attempts in the application. After all, a financial transaction requires some higher-level authorization, because if it didn’t it could represent a potential risk for the user and for the bank, compared to an online library containing only the basic user information. Then even in the worst scenario- data leakage to unauthorized people, won’t hurt the user as much.

4. How to apply the research findings in my project

Being a software engineer student myself, I often come to the point that I have to do some research and prototyping to see which ways of authentication and security fit my project best.

In my latest prototyping I tried to check every box in the list for an ethical, transparent, and secure application/website. Also being a customer to different services through various websites, I have many good examples on what one shouldn’t do when developing their product.

Regardless, I always at least ask for a second opinion from colleagues, teachers, and friends before deciding how to structure it. I believe feedback from people is an important aspect of the development because it gives you broader horizon and shows you viewpoints of different opinions, which eventually lead to more ethical and secure application.

5. Conclusion

In conclusion, implementing a tiered authentication system, with a strong emphasis on user empowerment, inclusivity, and compliance with GDPR, is crucial for ensuring the security and ethicality of an Online Book Library application.

While various authentication methods exist, a password combined with optional 2FA could be considered sufficient, emphasizing the need to balance security measures with user convenience and the nature of the application.

1. Sources

<https://www.orientsoftware.com/blog/software-development-security/>

<https://www.idrnd.ai/5-authentication-methods-that-can-prevent-the-next-breach/>

https://www.orientsoftware.com/blog/software-development-security/