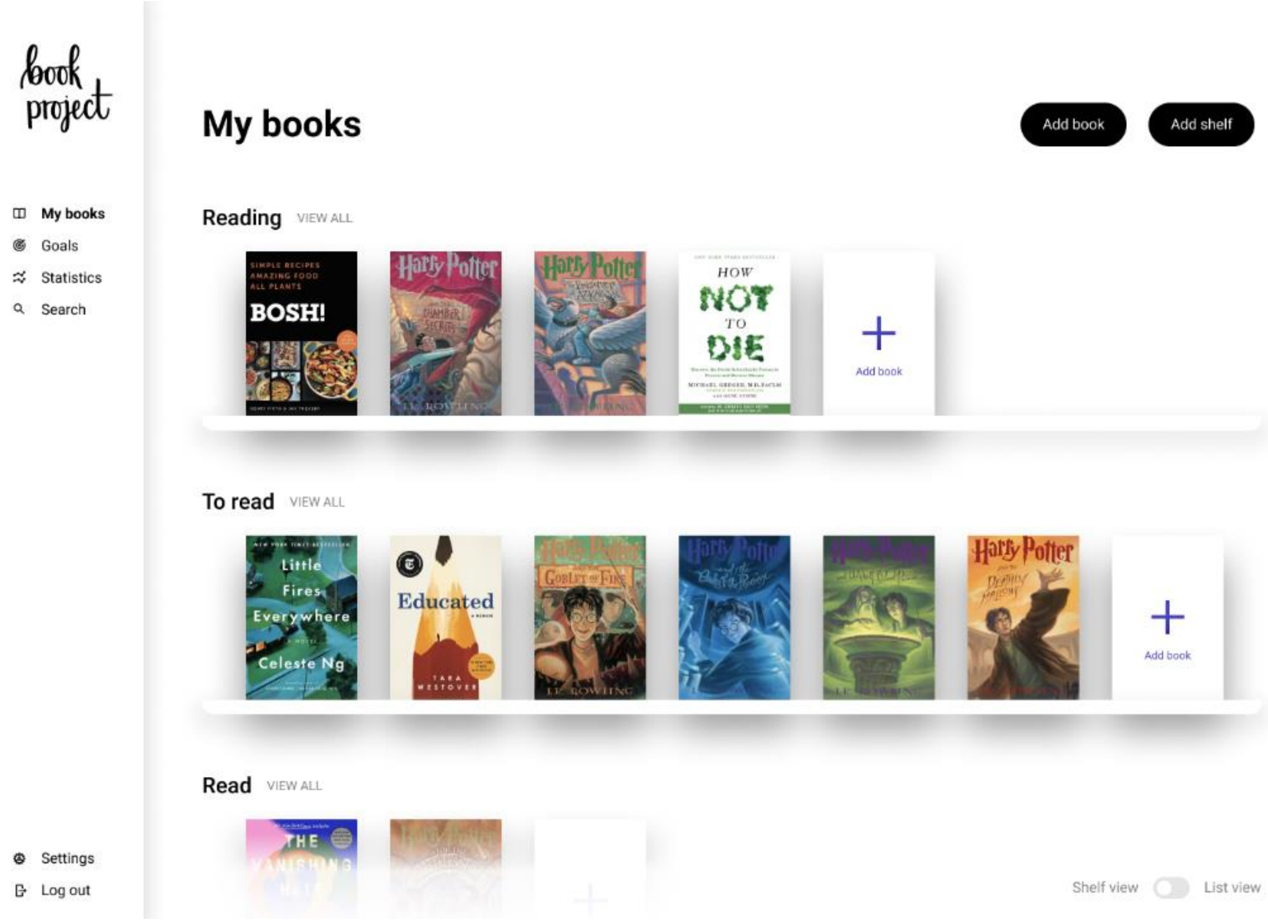
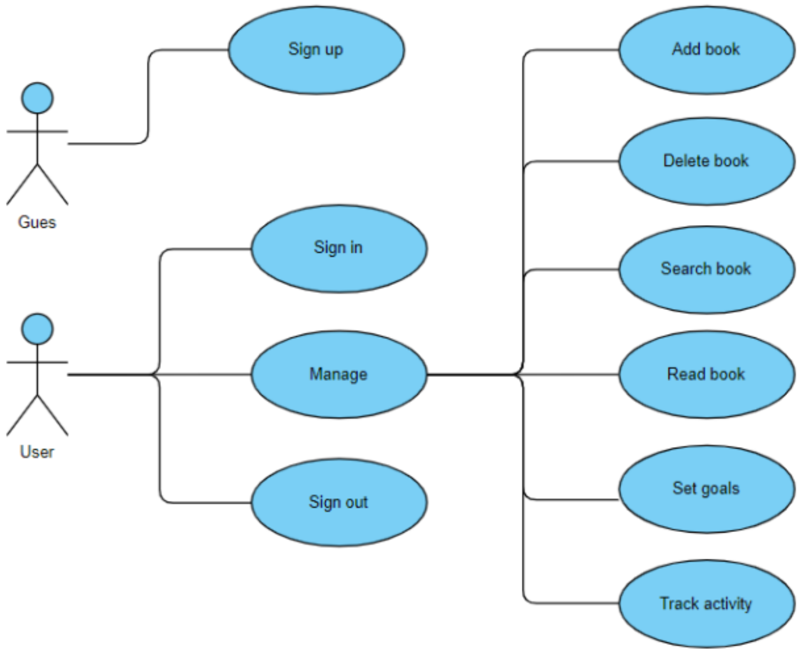
Project overview



Use case



Product features

The service will have the following major features:

- Authorization and authentication of users
- The ability to add and remove books
- Saving and sorting books
- The ability to set goals and track them
- The ability to track your activity

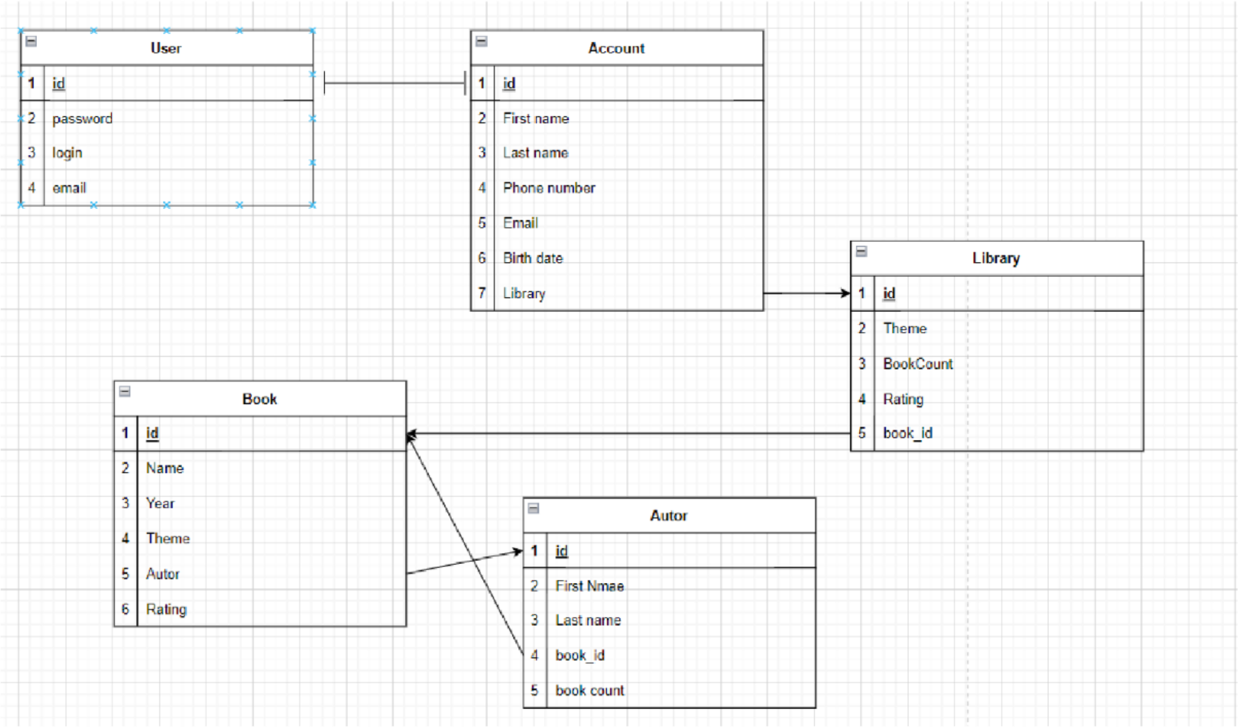
Basic technologies

The project will be developed using the following technologies:

- React.js;
- Java;
- MongoDB;
- Ajax;

Data model

ER-diagram



Description of entities

- User table stores login, email and hashed passwords.

- The account table stores additional personal information about

user

- The flats table stores the book category data (topic, number of books, rating and book id.

- The book table contains the book title, year, author, subject, and rating.

- The Author table contains more detailed information about the author of the book (name, surname, number of books and book IDs)

The application processes only your personal information (for example, first name, last name, phone number, email) if you are a simple user. If you want to add your book, then information about the book and everything related to it will be processed.

You can change personal data, for example:

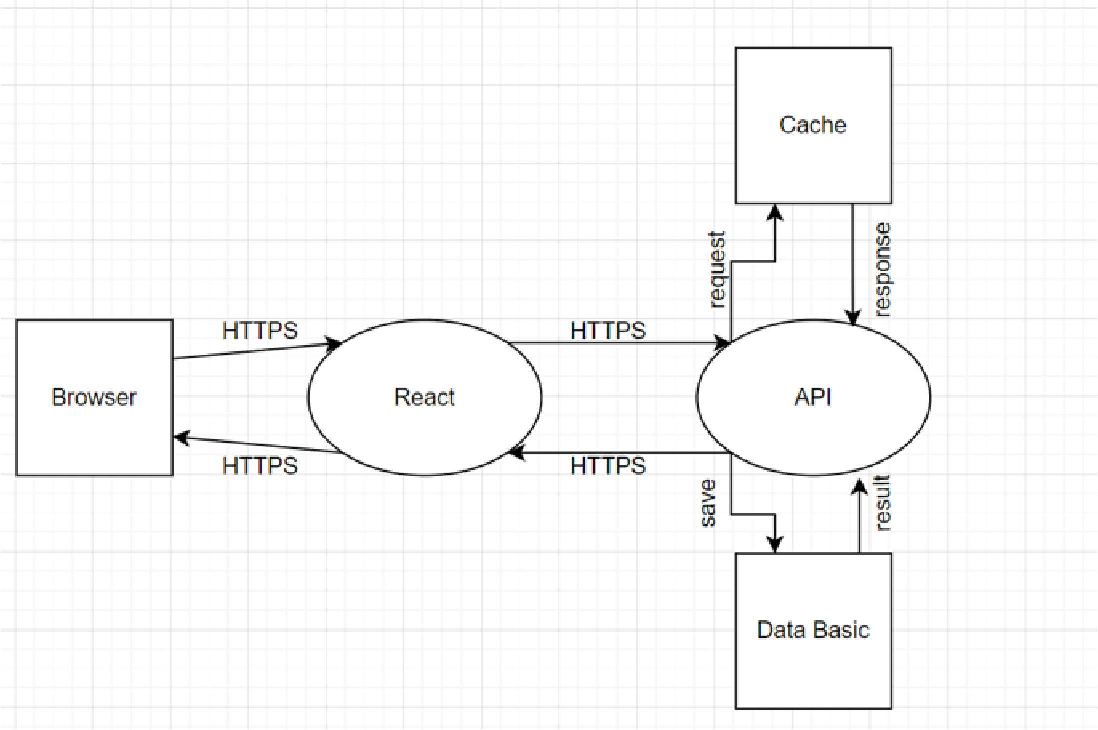
- You can change the First Name and Last Name
- You can change Your contact phone number
- You can change Email address

You can also delete the account at any time, and all user data will also be deleted.

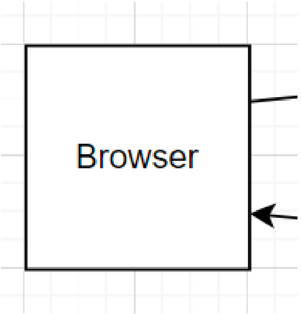
Security model

Threat model

Diagram

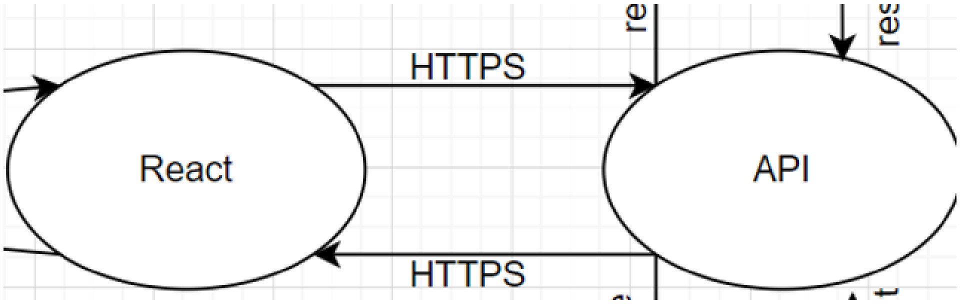


Interaction: in-browser manipulation



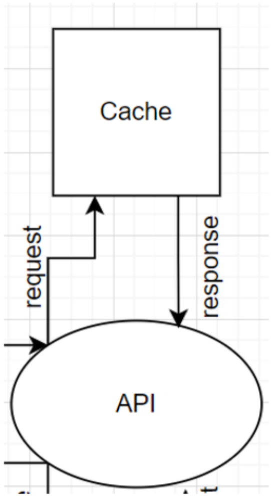
Category	Description	Control category	Effort
Spoofing	An adversary can steal application and service code on the client side.	Technology	High
DDOS	An adversary can spam system with account creation	Technology	Medium

Interaction: HTTPS



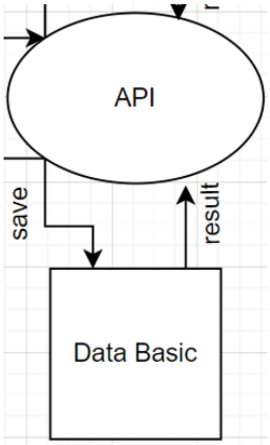
Category	Description	Control category	Effort
Spoofing	An adversary can steal data using man-in-the-middle-attack.	Data	High
Denial of service	An adversary may block access to the application or API hosted on React through a denial of service attack.	Technology	Medium

Interaction: Request/Response



Category	Description	Control category	Effort
Denial of service	An adversary may block access to the application or API hosted on API through a denial of service attack.	Technology	High
Denial of service	An adversary may assessing functionality of Cache API and change books information	Data	High

Interaction: Save

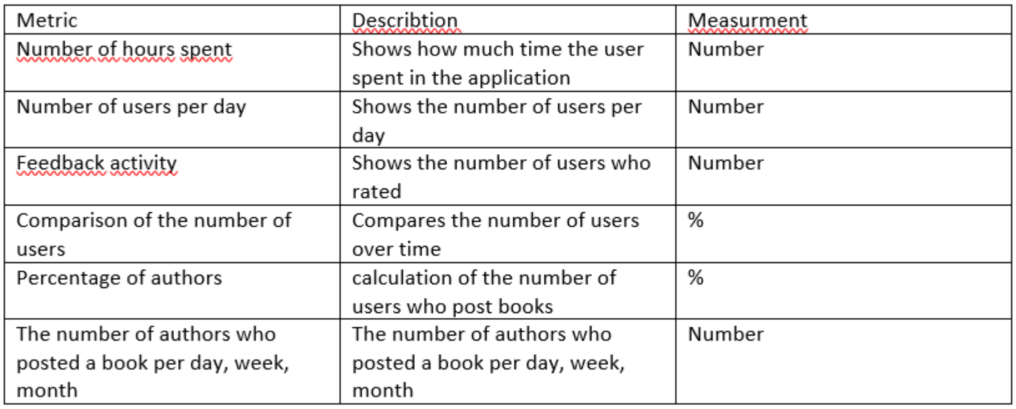


Category	Description	Control category	Effort
Elevation Of Privilege	An adversary may directly connect to DB from anywhere	Data	Medium
Elevation Of Privilege	If there is no restriction at network or host firewall level, to access the database then anyone can attempt to connect to the database from an unauthorized location	Data	Medium
Elevation Of Privilege	SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution.	Data	High
Elevation Of Privilege	An adversary may read unauthorized content stored in DB	Data	Low

Migitation plan of potential risks

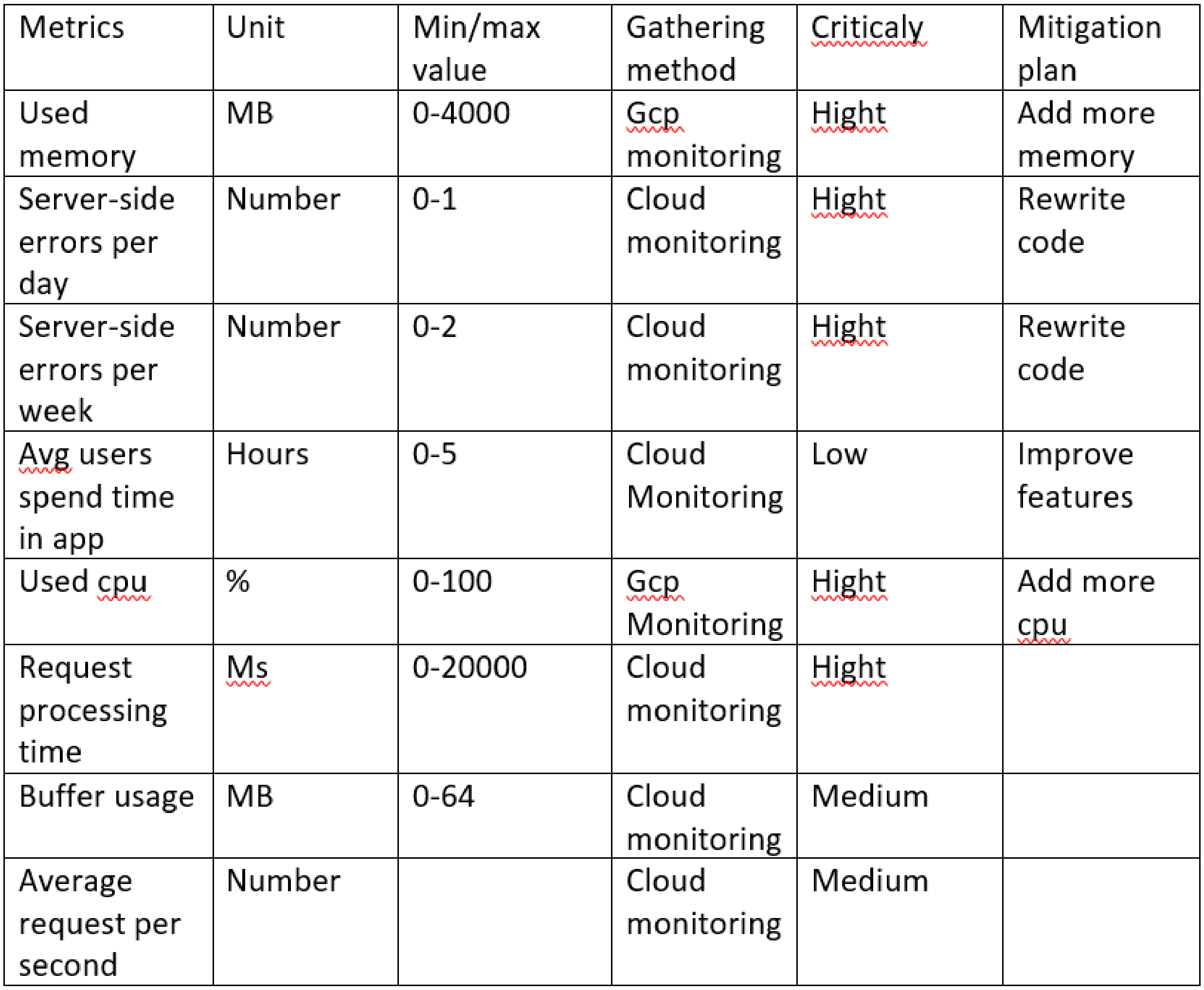
Risk	Solution
user data stealing (password, login, email)	provide access to db only for privileged accounts with admin rights
user account stealing(weak password)	ensure that user create strong password or generate it instead
account spamming	allow to create account only using gmail or phone number, or create strong verification during long time to avoid temporary mails accounts creating
sql injection and cross site scripting	not to use outdated components and 3rd sides libraries; provide additional penetration testing
DDOS	block ip addresses or add request timer with available amount of requests
code stealing	prevent using open source platform and use private repositories/ obfuscate client code
data spoofing	using https protocol instead of http

Analytics model



Metric	Describtion	Measurment
Number of hours spent	Shows how much time the user spent in the application	Number
Number of users per day	Shows the number of users per day	Number
Feedback activity	Shows the number of users who rated	Number
Comparison of the number of users	Compares the number of users over time	%
Percentage of authors	calculation of the number of users who post books	%
The number of authors who posted a book per day, week, month	The number of authors who posted a book per day, week, month	Number

Monitoring&alerting model



Metrics	Unit	Min/max value	Gathering method	Criticaly	Mitigation plan
Used memory	MB	0-4000	Gcp monitoring	Hight	Add more memory
Server-side errors per day	Number	0-1	Cloud monitoring	Hight	Rewrite code
Server-side errors per week	Number	0-2	Cloud monitoring	Hight	Rewrite code
Avg users spend time in app	Hours	0-5	Cloud Monitoring	Low	Improve features
Used cpu	%	0-100	Gcp Monitoring	Hight	Add more cpu
Request processing time	Ms	0-20000	Cloud monitoring	Hight	
Buffer usage	MB	0-64	Cloud monitoring	Medium	
Average request per second	Number		Cloud monitoring	Medium	