

Titel der Diplomarbeit

Dein Name

April 16, 2025

Abstract

Kurzfassung

Contents

Abstract	1
Kurzfassung	2
1 Introduction	5
1.1 Short description	5
1.2 Description of performed work	5
1.3 Methodology of the thesis	6
2 Tech Stack	7
2.1 PostgreSQL	7
2.1.1 Generel	7
2.1.2 Scheme of the database	7
2.2 node.js	8
2.3 Sequelize	8
2.4 express	8
2.5 React	8
2.6 PWA	8
3 Features	9
3.1 Login	9
3.1.1 Frontend	9
3.1.2 Backend	9
3.1.3 Error Handling and Security	10
3.2 Registration	10
3.2.1 Roles	10
3.3 Group System	11
3.4 Create Polls	11
3.4.1 Start-/ Endtime	11
3.4.2 Questions	11
3.4.3 Demographic Questions	11

3.5	Edit Polls	13
3.6	Voting	13
3.6.1	Disclosed Voting	13
3.6.2	Anonymous Voting	13
3.6.3	Public Voting	13
3.7	Results	16
3.7.1	CSV-Export	16
3.8	MyPolls	17
3.8.1	Polllink	17
3.8.2	Delete Polls	17
3.9	Accessibility	19
3.9.1	Tooltips	19
3.9.2	Screenreader	19
3.10	Styling	19
3.10.1	Generel styling	19
3.10.2	Responsive design	19
3.10.3	Individual styling	20

4 Summary 21

Chapter 1

Introduction

Link Gliederung: <https://www.diplomarbeiten-bbs.at/durchfuehrung/gliederung-der-diplomarbeit-und-formale-vorgaben>

1.1 Short description

The topic of this diploma thesis is creating a platform which supports different voting options like single, multiple or weighted choice. Additionally there should be a Login system with different roles to administer and create or delete polls and one where the user can simply vote for the polls he's included in. Furthermore there an option to disclose the results and who voted for which answers. The database should run on a remote server and be accessed by an API.

The reason we chose this topic is because our supervisor is part of the LMP party and they couldn't find an appropriate platform to vote on party intern problems and topics. Hence he approached us and suggested we write our diploma thesis on a voting platform.

1.2 Description of performed work

Our aim is to provide a website where different organizations can create and publish polls for their members. Since our finished work will be open source, everyone who wants to create polls will benefit from our work.

We chose to accept the LMP as our partner, because they brought up that there isn't a platform that supports all the features they need. Moreover can they give us feedback of the real life application so we can adjust the features to a user organization. During the development of our work we had monthly meetings with the LMP to discuss the progress. Because we decided

to develop our software in an agile way the discussions we had with them also helped so we could focus on the more important features first and implement elements of lesser importance later.

1.3 Methodology of the thesis

At first we had to decide on a tech stack. After careful consideration we decided upon a PostgreSQL database, a backend of node.js, sequelize to perform database operations and express to write APIs so we can connect with our frontend. Our frontend is based on React and we also included a PWA. After this decision we began with a simple input and output from front- to backend so ensure we all understood how each part is connected to each other. The next step was implementing the first features. We split the elements in different components so we could work separately and efficiently, e.g the single choice is split in create the poll, display the poll, vote, and show the results. Reasons we chose this tech stack and a thorough description of each function our work has will be in the main part.

Chapter 2

Tech Stack

2.1 PostgreSQL

2.1.1 General

PostgreSQL was chosen as the relational database management system for this project due to its robustness, scalability and strong support for advanced data types and queries. The decision to utilize PostgreSQL was further supported by its user-friendly design, extensive and well-maintained documentation, and its widespread adoption as one of the leading open-source relational databases.

The installation was also simple because of the detailed install guide provided by multiple sites like **w3schools**. Before the installation certain configuration had to be done such as: specify the storage directory, select a password, set the port the server should listen on. To create the first database the SQL shell of PostgreSQL was used in the beginning. But after that the preferred tool was **pgAdmin 4**, an popular and feature rich Open Source administration and development platform for PostgreSQL, to manipulate data or view schemes of the database.[5]

For this project it was essential to have a stable and robust system in the backend that can handle a bigger amount of data efficiently.

2.1.2 Scheme of the database

The database consists of 13 tables, with "UserPolls" and "QuestionAnswers" functioning as intermediary tables that facilitate many-to-many relationships between the core entities.

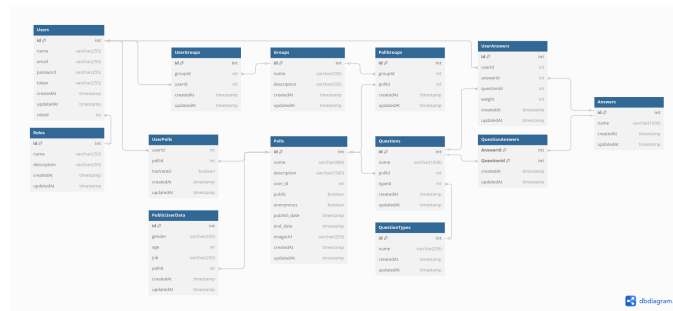


Figure 2.1: Entity Relationship Diagram

2.2 node.js

2.3 Sequelize

2.4 express

2.5 React

2.6 PWA

Chapter 3

Features

3.1 Login

The login feature is essential for our application, as users need a secure and reliable way to authenticate themselves and gain access to their accounts. It consists of two main functionalities: the login itself and also the logout. Additionally, we have implemented user-friendly error handling to enhance user experience as well as security.

3.1.1 Frontend

The frontend component of the login feature uses React's built-in `useState` hook in order to manage the input username and password and store them in the component's state temporarily. After submitting the login form, the input data is sent to the backend API via a POST request.

The password is sent to the backend in plaintext over HTTPS. It is not encrypted on the client side, because HTTPS already provides built-in encryption and also protects against interception or man-in-the-middle attacks.

3.1.2 Backend

The backend receives the login request through a predefined API route that forwards the data to the `handleFetchLogin` function in the user controller. It extracts the username and password from the request body and passes them to the `fetchLogin` function in the user service.

This function first checks if a user with the provided username even exists in the database. If no user is found, it returns an error message stating

that either the username or password is invalid. We intentionally chose to not specify which of the two parts is incorrect in order to prevent attackers from being able to determine whether a username exists in the system. This provides protection against user enumeration attacks.

If a user is found, the provided password is then compared to the hashed password stored in the database using bcrypt's comparison method, `bcrypt.compare()`. In case the passwords do not match, the same error message mentioned above is returned to the frontend.

However, if the password is correct, the backend returns a response containing a success indicator, the user's unique ID (`userId`), their username, the assigned role ID (`roleId`), and the name of the role (`roleName`).

3.1.3 Error Handling and Security

Error handling is implemented consistently across both frontend and backend to ensure security and user-friendliness. If a login attempt fails, whether due to an incorrect username, password, or both, the system always returns the same general error message. This prevents attackers from determining whether a specific username exists in the system.

Sensitive data like passwords is handled securely. Passwords are not stored in plain text. Instead they are hashed using bcrypt before being inserted into the database. Furthermore, communication between frontend and backend is encrypted through HTTPS. This ensures that all transmitted data remains private and protected from unauthorized access.

3.2 Registration

3.2.1 Roles

Implementing a role-based system with three distinct roles - "Admin," "Poweruser," and "Normal" - is crucial for the functionality and security of the application. By assigning permissions flexibly, a clear hierarchy is established, enhancing both user experience and data integrity. Admins are granted full control over the application, while Poweruser enjoy extended privileges for managing polls. Normal users can seamlessly participate in polls and view results without jeopardizing sensitive functionalities. This structure facilitates efficient task delegation and scalability, allowing the application to be easily

expanded with additional roles in the future. The role system thus significantly contributes to the security, organization, and user-friendliness of the polling application.

3.3 Group System

3.4 Create Polls

3.4.1 Start-/ Endtime

3.4.2 Questions

Single Choice

Multiple Choice

Weighted Choice

3.4.3 Demographic Questions

To gather the data of our public voters, the implementation of demographic questions was crucial. This feature is only available for public polls since the created user would be part of the organization using our project and therefore have the data already. If the users is not part of the organization there is still the option to contact them via the e-mail used for the registration. Since most of these questions are similar for every poll, a modular system where questions can be created, added, removed and changed is the best solution. Figure 3.1 shows the demographic question in create polls. The options and functionality of these questions are the like ones described in the previous sections, with the difference that weighted is not an option, since demographic data is more like a fact less an opinion.

The new part for this feature is the search bar. For this the "Select" component of "react-select" is used. The components' controllable state props and modular architecture allows "isMulti" to select multiple options or "isSearchable" to search. These features, allow easy implementation and an already styled search bar in the project. [10]

The database structure for the demographic questions is similar to the standard ones. The table "PublicQuestions" is used to store the question specific data like name and type. To enable the reuse of questions on different polls "PublicQuestions" is in an many-to-many relationship with "Polls"

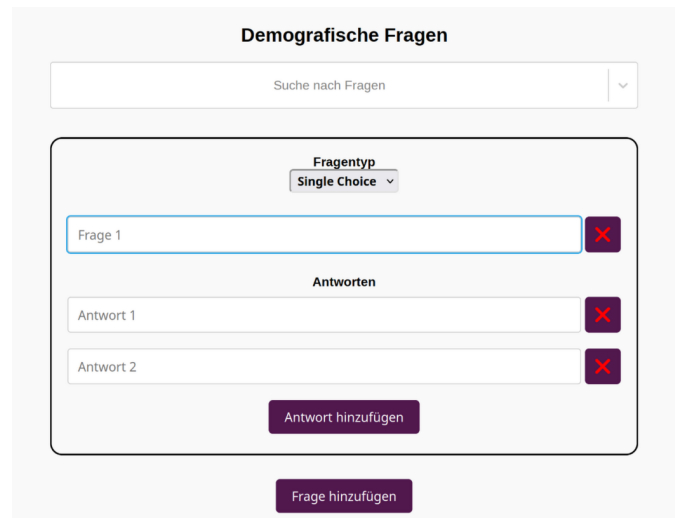


Figure 3.1: Create Demographic Question

through "PublicPollQuestions". Answers are stored within the table "PublicAnswers", which is connected to "PublicQuestions" via "PublicQuestionAnswers". This relation is also many-to-many since the options yes or no for example would be used in multiple questions.

For the select every existing question with its answers is fetched from the database and stored within an array. The options are then mapped with the value being id and the label as name of each element. To display the selected options they are mapped through and use the same functions as the standard ones used for the poll. When saving these questions a problem arises, as the selected ones are already stored in the database and possibly changed. To handle this a findOrCreate 3.2 is used to get the existing questions and answers or create new ones. This function also returns each instance found or the created one. With this the question and answer ids can be used for the many-to-many relationship. [4]

```

1  let [createdQuestion, created] = await
    ↪ PublicQuestions.findOrCreate({
2    where: {
3      name: question.name,
4      typeId: questionTypeId,
5    }
6  });

```

Figure 3.2: findOrCreate PublicQuestions

3.5 Edit Polls

3.6 Voting

3.6.1 Disclosed Voting

3.6.2 Anonymous Voting

3.6.3 Public Voting

The public voting allows users without an account to vote. With this feature a wide range of people can be questioned in street surveys or through a shared link. This poll type has two sections, the normal and demographic questions. The order of these plays a major role. Römermann mentions trust, benefits of the demographic data and the ability to abstain. All of these factors have to be taken into one's account when creating these questions. The article also mentions, that at the beginning of a survey the motivation is high and the demographic data are answered, but the trust in full anonymity is decreased. Therefore the author states it is best to put these questions at the end. [7]

Poll Questions

In public voting, since users cannot select a poll themselves, it's important to handle cases where the poll is accessed via a direct link outside the allowed time frame. To keep things simple, a short message — "Poll not available" — is displayed in such cases. If the site is accessed within the designated start and end dates, the questions are shown, similar to those in disclosed and anonymous voting. The main difference in this voting method lies in the submit button. Its function is only to change the display so that demographic questions are shown.

Demographic Questions

After the poll is completed, the demographic questions linked to it are displayed. These questions follow the same visual style as those in the other sections. Once submitted, the submit button becomes greyed out and disabled. A short thank-you message, along with a link to the organization's website, is then shown. Similar to the poll questions, the key difference here lies in how the submit button behaves. Before sending the data, the system checks whether the user has already voted. If not, the responses to both the poll and demographic questions are sent to the backend API via a POST request. The service processes these answers and inserts them into the corresponding database tables.

Vote Integrity

A major problem when having anonymity and no accounts is the data integrity. Without the ability to store information about a voter in the database to check for multiple votes, it is important to prevent them from voting multiple times. Completely avoiding this problem is nearly impossible, but to ensure no problems arise we chose two different security measures.

To prevent fraudulent activity, spam, and abuse with bots, Google reCAPTCHA is integrated into the application. To implement this a key pair is generated, one for the site and a secret key. The site key is used to integrate the reCAPTCHA service into the frontend. The secret key facilitates secure communication between the backend server and the reCAPTCHA system to validate user responses. To maintain security the keys are stored in an env file. For this whole process the invisible option is checked to prevent the flow of the voting being disturbed.[3]

3.3 shows how the backend handles the CAPTCHA request. The token, the site key, is sent from the frontend through the request body, while the secretKey is accessed via the process.env environment variable. To maintain readability, the URL is defined and the query string includes both keys. Then these parameters are sent to Google's endpoint to validate the user interaction. The score in Google's response indicates how likely a user is human. Therefore, before returning a successful response to the frontend, the score is checked. The code also handles the cases where the request results in an error or the score is too low. [3]

```

1 app.post('/verify-recaptcha', async (req, res) => {
2   const { token } = req.body;
3   const secretKey = process.env.RECAPTCHA_SECRET_KEY;
4   const url = `https://www.google.com/recaptcha/api/
5   siteverify?secret=${secretKey}&response=${token}`;
6   try {
7     const response = await fetch(url, {
8       method: 'POST',
9     });
10    const data = await response.json();
11    if (data.success && data.score > 0.5) {
12      res.json({ success: true });
13    } else {
14      res.json({ success: false, message: 'Verification failed'
15        ↪ });
16    }
17  } catch (error) {
18    console.error('Error verifying reCAPTCHA:', error);
19    res.status(500).json({ success: false, message: 'Server error'
20      ↪ });
21  }
22 });

```

Figure 3.3: reCAPTCHA backend

Cookies are small pieces of data stored locally on a user's device by their browser. They are commonly used to save user-specific information, such as usernames or passwords, to enhance the web browsing experience.

Other common use cases include:

1. Session Management: Allows a website to remember user behavior and preferences across sessions.
2. Personalization: Enables websites to tailor content, such as language settings or recommended items, to individual users.
3. Tracking: Often used in e-commerce to maintain a shopping cart while users navigate through different pages of a site.

In all these scenarios, the data is stored locally on the user's device [6]. On this platform, however, cookies serve a more specific purpose: to store a boolean flag indicating whether a user has already voted. Figure 3.4 illustrates how the cookie is stored in the browser. The cookie's expiration is set to the poll's end date, ensuring it is automatically removed once voting closes.

Name	Value	Domain	Path	Expires / Max-Age
pollSubmitted	true	localhost	/	Wed, 16 Apr 2025 22:00:00 GMT

Figure 3.4: Cookie stored in the browser

The cookie is set only after the voting request is successfully processed. This order is crucial, as vote submissions can occasionally result in errors. If the cookie were set before confirmation, users could be wrongly prevented from resubmitting. By storing the cookie only after a successful vote, users can correct and resubmit their answers when needed.

This method is not entirely secure. If someone knows where the cookie is stored and how to access it, they can delete it and vote again. Still, this setup addresses most common threats to the integrity of the poll.

3.7 Results

3.7.1 CSV-Export

To allow for the further analysis and documentation of the poll results, a CSV export functionality was implemented. This export provides a structured overview of all user responses, including additional metrics such as the number of votes per answer and the average weight for weighted questions.

The logic is handled in the **csvExportController.js** controller. Upon receiving a request, the system retrieves all relevant data for a given poll by its ID, including associated question, answers, and question types. The raw voting data is processed to count the number of responses per answer and to calculate the average weight if applicable. Special care is taken to distinguish between different types: for instance, "Single Choice" questions ensure that only one answer per user is counted, while "Weighted Choice" questions include the weight value in the computation.

The processed data is then converted into a structured CSV format using the `json2csv` library. The final file includes columns such as Poll Name, Question, Question Type, Answer, Vote Count and Average Weight, and can be downloaded directly by the user. This feature ensures transparency and enables further statistical evaluation using external tools like Excel.[1]

3.8 MyPolls

3.8.1 Polllink

To make sharing of the Surveys easier, a QR code generation was implemented. This was done using the React component `"qrcode.react"` which requires the link to the poll.[2]

3.8.2 Delete Polls

The deletion of polls is crucial for two main reasons: first, to ensure that all associated data of a survey can be safely removed when necessary and second, to determine when a poll is still eligible for deletion. In this case, the deletion of polls is strictly limited to those that have not yet received any user votes.

This constraint ensures the integrity of the data and avoids loss of user-generated information, which could distort statistical analysis or transparency within the system.

To maintain data consistency, the deletion process is implemented as a transaction. This guarantees atomicity, meaning that either all steps of the deletion process succeed or none do - preventing partial data deletion and potential corruption. Sequelize's transaction management is used here to wrap the entire process in a rollback-safe structure. [4]

The deletion logic performs the following steps

1. Validate that the poll exists.
2. Fetch all related questions and their IDs.
3. Check if any user answers exist for these questions. If so abort the operation with an error.

4. Remove the many-to-many relations between answers from the "QuestionAnswers" table.
5. Delete the associated answers.
6. Delete the questions.
7. Delete any group relations in the "PollGroups" table.
8. Finally, delete the poll itself.

```
1  const deletePoll = async (pollId) => {
2    const transaction = await sequelize.transaction();
3    try {
4      ...
5      await PollGroups.destroy({
6        where: { pollId },
7        transaction,
8      });
9      await Polls.destroy({
10       where: { id: pollId },
11       transaction,
12     });
13     await transaction.commit();
14     return { pollId, questionsDeleted: questionIds.length };
15   } catch (error) {
16     await transaction.rollback();
17     throw error;
18   }
```

Figure 3.5: Example for a Sequelize transaction

Using Sequelize's transaction mechanism not only helps to avoid data inconsistency, but also ensures that no information is accidentally deleted once users have participated in a poll. This feature is particularly important in environments where transparency and trust are key, such as in political or organizational voting systems.

3.9 Accessibility

3.9.1 Tooltips

3.9.2 Screenreader

3.10 Styling

3.10.1 Generel styling

The styling of the application was done later in the making process, because only then it was demanded by the customers. The same applies to the color scheme which has two main colors: Yellow and Purple.

To ensure consistency of the palette user defined characteristics from CSS where used to assign variables for each main color. [9]

```
1  :root {  
2    --primary-color: #51184e;  
3    --secondary-color: #F9BB03;  
4    --primary-hover-color: rgb(163, 131, 168);  
5  }
```

Figure 3.6: Variables of the main colors

Those variables where then used in each element of where it was needed. Therefore changing the color scheme to a different one is less afford for the end user.

The basic structure of the page is split into three sections: header with navigation, main with content and footer with imprint and privacy policy. The style is based on the client's homepage therefore the standard background is purple but of the content it still is white to ensure readability. [8]

3.10.2 Responsive design

Responsive design is essential nowadays because users access websites from a wide variety of devices - phones, tablets, laptops and desktops - each with different screen sizes and resolutions. It ensures a seamless, user-friendly experience across all platforms, which improve engagement and accessibility.

To ensure responsiveness in each section of the application, "@media CSS at-rule" was used to apply different styles based on the screen size or device characteristics. This approach allows the layout, font sizes and element spacing to adapt dynamically, creating a smoother experience for users on any device. The navigation bar was designed with media queries to transform into so-called "burger menu" when the screen width falls below a certain threshold. This ensures usability on smaller devices like smartphones because the elements within the navigation get displayed in the menu now.



Figure 3.7: Navigation



Figure 3.8: Burger menu

3.10.3 Individual styling

Chapter 4

Summary

Bibliography

- [1] Node.js Contributors. *json2csv*. URL: <https://github.com/juanjoDiaz/json2csv> (visited on 04/13/2025).
- [2] React Contributors. *qrcode.react*. URL: <https://www.npmjs.com/package/qrcode.react> (visited on 04/13/2025).
- [3] React Contributors. *react-tooltip*. URL: <https://github.com/ReactTooltip/react-tooltip?tab=readme-ov-file> (visited on 04/15/2025).
- [4] Sequelize Contributors. *Sequelize Documentation*. URL: <https://sequelize.org/docs/v6/core-concepts/model-querying-finders/> (visited on 04/09/2025).
- [5] W3Schools Contributors. *PostgreSQL - Install Introduction*. URL: https://www.w3schools.com/postgresql/postgresql_install.php (visited on 04/15/2025).
- [6] kaspersky. *What are Cookies?* URL: <https://www.kaspersky.com/resource-center/definitions/cookies> (visited on 04/16/2025).
- [7] Carina Römermann. *Was ist bei soziodemografischen Angaben in Befragungen zu beachten?* URL: <https://www.rogator.de/soziodemografischen-angaben-mitarbeiterbefragungen/> (visited on 04/09/2025).
- [8] tbd. *Liste Madeleine Petrovic*. URL: <https://liste-petrovic.at/> (visited on 04/13/2025).
- [9] tbd. *Verwendung von CSS-Benutzerdefinierten Eigenschaften (Variablen)*. URL: https://developer.mozilla.org/de/docs/Web/CSS/CSS_cascading_variables/Using_CSS_custom_properties (visited on 04/12/2025).
- [10] Jed Watson and contributors. *React-Select*. URL: <https://www.npmjs.com/package/react-select> (visited on 04/09/2025).

List of Figures

2.1	Entity Relationship Diagram	8
3.1	Create Demographic Question	12
3.2	findOrCreate PublicQuestions	13
3.3	reCAPTCHA backend	15
3.4	Cookie stored in the browser	16
3.5	Example for a Sequelize transaction	18
3.6	Variables of the main colors	19
3.7	Navigation	20
3.8	Burger menu	20