Project 2: TeamNote

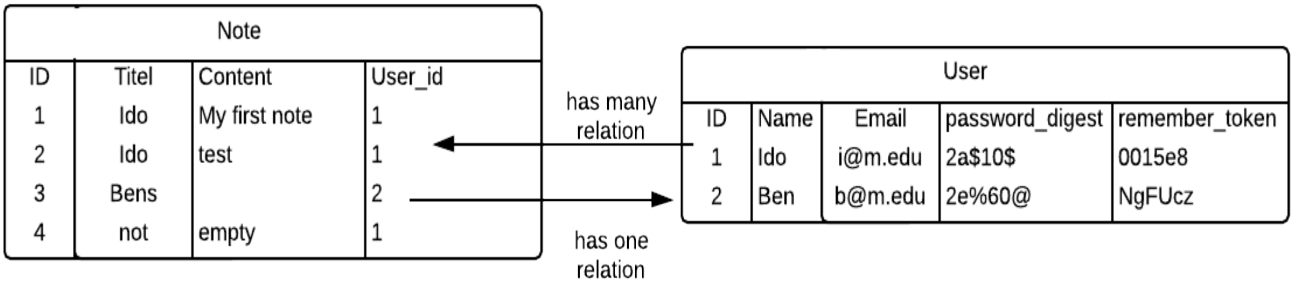
Design Analysis
Ido Efrati
6.170 Fall 2013
October 6, 2013

1. Overview:

TeamNote phase 2 is a browser-based note-taking application that allows users to create and organize textual notes, save them and access them. Phase 2 introduces additional functionality to the project, accounts and sessions. Users can create an account and create, edit, delete and show their notes. Meaning users can only access their notes. Currently the application does not support view permissions to other users (to be added in phase 3 of the project).

2. Concepts

2.1 Database design and relations



Note

ID	Titel	Content	User_id
1	Ido	My first note	1
2	Ido	test	1
3	Bens		2
4	not	empty	1

User

ID	Name	Email	password_digest	remember_token
1	Ido	i@m.edu	2a10	0015e8
2	Ben	b@m.edu	2e%60@	NgFUcz

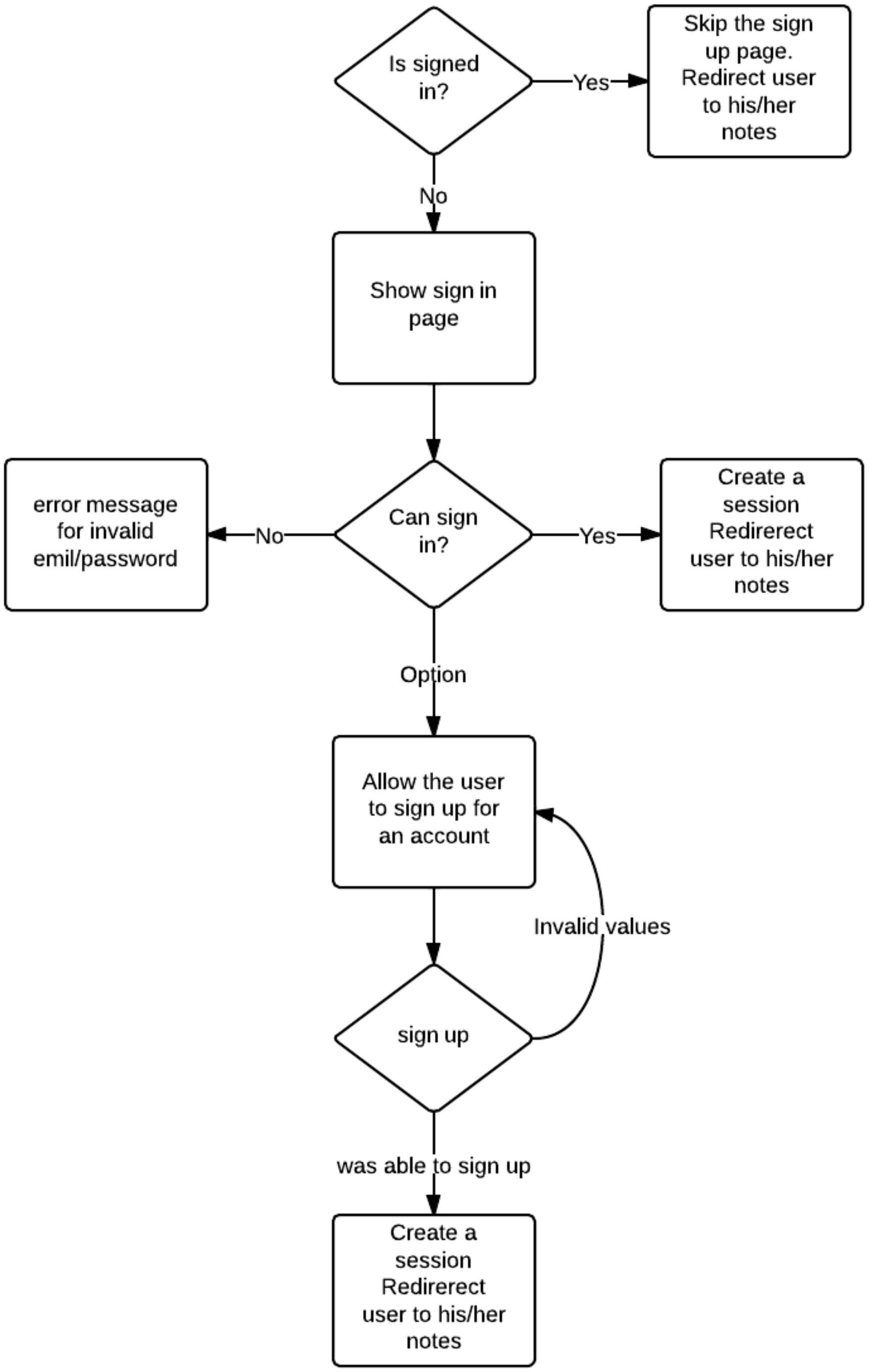
As seen in the above diagram TeamNote consists of two tables, a note table and a user table.
A user has a name, an email, and encrypted password to protect from attacks, and an encrypted session token to prevent from sessions attacks. Most of the validation is performed only at the model level (presence of required field, and correct format), but uniqueness validation is performed both on the model level and on the database level. The reason behind the double uniqueness validation

is to prevent a duplicated creation of an entry, if the user clicks the sign up button twice with a slow Internet connection.

A note has a title, content and an owner (the user who created the note). A user can edit the title and the content of the note but cannot change an owner of a note. The owner field stored as an integer the corresponded to the primary key of a user in the user table.

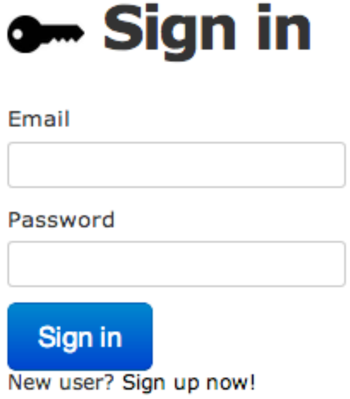
Finally, as demonstrated by the above diagram a user has a *has many* relation to notes, and a note has a *has one* relation to a user.

2.2 Users and session

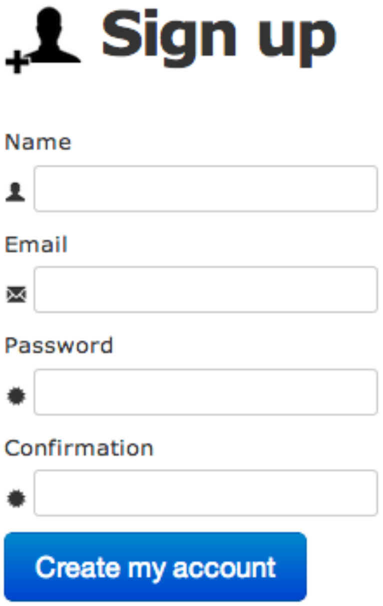

Is signed in?
Yes
Skip the sign up page. Redirect user to his/her notes
No
Show sign in page
error message for invalid emil/password
No
Can sign in?
Yes
Create a session Redirerect user to his/her notes
Option
Allow the user to sign up for an account
Invalid values
sign up
was able to sign up
Create a session Redirerect user to his/her notes

In phase 2 users can create their own accounts, sign in to TeamNotes, and maintain a session. When a user first accesses the server, the server will check if the user is already signed in. If the user has a working session (stored in the user's table under remember_token), the user will be redirected to his/her notes.

Otherwise, the user will have to either sign in or sign up. If the user has an account he or she can use the sign in option:



Otherwise, if the user wishes to create a new account he or she can use the sign up form:



Finally, when the user sign out of the system, the session will be cleared the remember_token value will be removed from the table.

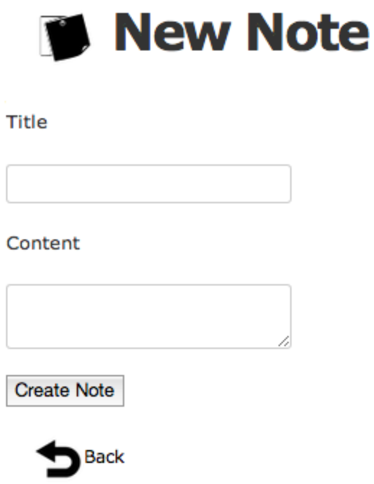
<u>2.3 Notes</u>

A note consists of three fields:

<u>Title</u> - the note title stored as a string

<u>User</u>- the name of the owner, the owner's value is being set during the creation of the note, and is based on the currently logged in user.

<u>Content</u> – the content of the note. A text area, since a string is limited in its length and a user might want to write a longer note.



3. Functionality and features

3.1 Features:

TeamNote currently supports the following features:

Create – allows the user to create a new note as long as the user specifies the required fields (see section 3.2)

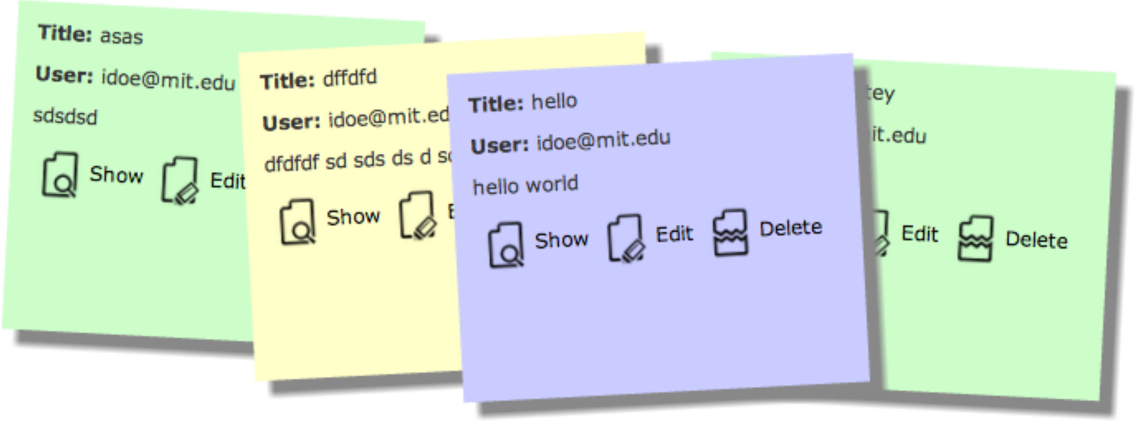
Show – allows the user to access an existing note and read it.

Edit – allows the user to edit an existing note. Currently the user may change the name of the user who created the note. A user will not be able to save an edited note if required fields are left empty.

Delete – allows the user to delete an existing note. Will prompt the user with a verification window.

Back - sends the user to the main page, where he or she can see all the existing notes

Sign up – users can create an account on TeamNote.
Sign in – users can sign in to TeamNote if they have an account.
Sign out – users can clear their session. After a sign out a user will be require a new sign in.
Dragging notes – notes can be dragged around. This feature was added in an attempt to learn how to integrating jquery/javascript into rails, and how to overcome issues with turbolinks.



Title: asas
User: idoe@mit.edu
sdsdsd

Title: dffdfd
User: idoe@mit.ed
dfdfdf sd sds ds d s

Title: hello
User: idoe@mit.edu
hello world

ey
it.edu

4. Security

3.1 validations:

In order to create a note, a user must specify a title. If a user tries to create a new note without specifying the above fields, the application will prevent the user from creating the note. The reasoning behind this design decision is that every note has to have a creator, and a note cannot be empty (there is no point in adding empty entries to the table). From a better user interface perspective, the content field is optional. A user might want to create a short note that can be summarized only by its title (for example, “submit 6.170”). In this case the content will be redundant if the user does not wish to add anything else.

In order to create a new account a user must specify a username, email address, password and password confirmation. As mentioned earlier email address and username have to be unique. Any attempt to create a user without the above fields or with values that are not unique will prompt the user with an error message.

3.2 authentications

3.2.1 user authentication

When users tries to log in the server will try to authenticate their email address and password with the email address and the encrypted password that are stored in the database. Only if the two match the user will granted access and will be assigned a session.

3.2.1 session authentication

When the server verifies if a user is already signed in, it will compare the encrypted session that is stored in the user's table under remember_token to an encrypted version of the local cookie. Only if the two match a user will be granted access to his or her notes. By doing so the server guarantees that the cookie was not tempered with to allow unauthorized access.

3.2.3 access control:

Users cannot temper with the URL in an attempt to gain access to a note that they do not own. If a user tries to access a link before a session was establish he or she would not be able to access the site. If the user is already logged in and tries to change the URL path to access a different note (i.e. changing the id value in the URL) he or she will be redirected to a *page cannot be found.*

4. Testing

The following manual tests were performed on the application:

Positive tests:

Category: valid use of the application. Expected result: the user will be able to perform the require action.

1) Creation of a new note with values in all fields.
2) Creation of a note with values only in the title and user fields.
3) Creation of a note with the same title or with the same user.
4) Editing of a note to change its title/user/content.
5) Showing an existing note.
6) Deletion of an existing note.
7) Going back from every page to the main page.
8) Going back in the middle of an edit, verify that the content was not changed.

Category: valid use of the application. Expected result: the user will be able to sign in, sign up, and sign out.

1) Sign in with a valid email and password
2) Sign up with all required values
3) Viewing only notes that were created by a user
4) Accessing TeamNote after a session was establish
5) sign out and verify that the session was removed from the DB.

Negative tests:

Category: Invalid creation/editing of a note. Expected result: the user will not be able to create a note or save an edit of a note.

1) Creation of a note without a value in the title field.
2) Creation of a note without a value in the user field.
3) Creation of a note without values in both a title field and user fields.
4) Editing and saving of a note without a value in the title field.
5) Editing and saving of a note without a value in the user field.
6) Editing and saving of a note without values in the user and title fields.

Category: Invalid creation of a user, invalid sign in, and invalid access control. Expected result: the user will not be able to access TeamNote

1) Trying to sign in with invalid email/password.
2) Trying to sign up with an existing user.
3) Trying to sign up without specifying all required fields.
4) Open two windows in an attempt to access the system with two different users.
5) Changing URL values after a successful login , to gain access to notes that the user does not own.
6) Changing the URL values to bypass the sign in process.

5. Attribution

Images are attributed to Vytautas Ajechnavicius from the Noun Project.
http://thenounproject.com/vytautas.alechnavicius/

Notes image - evernote.com/market/feature/3m?sku=MMMP00102