**Web Applications:**

Local

Overview

The door lock system uses the on-board Wi-Fi chip as a server to obtain the web site. The website is simple and contains three possible options: enroll user, delete all users and configure Wi-Fi connection. When the physical door is opened, the authorized personnel can connect to the on-board Wi-Fi chip through her internet-enabled devices and gain access to this interface. When the authorized personnel decides to enroll a new fingerprint to the system by pressing the button beside the solar panel, instructions will show on the web page as loaded from the micro-controller via the Wi-Fi chip.

Features

Enroll - When the user clicks on the plus sign, it indicates that the user wants to enroll a new fingerprint. This is only possible when the door is opened and that the Wi-Fi is in server mode. The interface will display instructions telling the user to place or remove her finger at appropriate times until the final message showing that the process is complete and that the users should now be updated on the web server. Each new users will be added to the queue and sent to the web server every thirty minutes such that the users cannot forcibly add user outside of the thirty minute block.

Delete - When the user clicks on the minus sign, it indicates that the user wants to delete all users from the fingerprint reader. The microcontroller simply removes all user from the system along with the fingerprints saved on the fingerprint reader.

Set Wi-Fi - When the user clicks on "Set Wi-Fi", it indicates that the user wants to edit the network connection. The user can simply enter a new network SSID and its corresponding password. Next time the thirty minute update occurs, the Wi-Fi will attempt to connect to the new network to reach the internet.

User Interface Program

This contains an HTML script with consists of CSS and JavaScript. The CSS simply adds color and resizes the element to fit the screen of the internet enabled-device. The JavaScript code uses XHR to receive responses and display them on the screen in the appropriate spots. The code is triggered when the webpage has a state change in the browser, in this case, receiving an HTTP response. This is handled internally by the browser itself such that the state is equal to 4 when the data is ready to be read. The same code is triggered recursively as long as the received message does not end with a dollar sign. The dollar sign indicates that the process of enrolling a fingerprint, deleting a user, etc has been interrupted or is over. That way, the web page will cease the continuous requests which is used to step through the process of enrolling, deleting the user and setting the Wi-Fi. The script fires an HTTP request to the server on the Wi-Fi chip asking for the corresponding page. Set Wi-Fi requests the update synchronization which contains extra information including time, schedules and deleted users. The protocol between the embedded system and the internet enabled-device is a query string variables delimited by the ampersand symbol which abides to the standard HTTP.

On the Internet

Overview

The website serves as an interface for the smart door lock as a mean to provide remote access to the system. It has the basic profile registration such as email and password authorization. In order to register, the user must provide the product ID included in the package which would come along with the door lock.

After registration, the users can enter the website and access features like add, delete users and accounts. For usability, we have also included a mechanism for password reset and forget password option. For security measures, there are no direct ways to modify the authentication on the physical system. Any action taken will be synchronized with the physical system to ensure stability and consistency. The users can choose to modify access schedule of each users, delete or rename them if they are admin of those certain users - permitting them to do so.

The user information is visualized using styled and animated HTML elements, located in the two main panels at the right hand side of the page. There is a menu on the left showing options to add users, delete accounts and more. When these options are selected, the main panels will display the information relevant to the options.

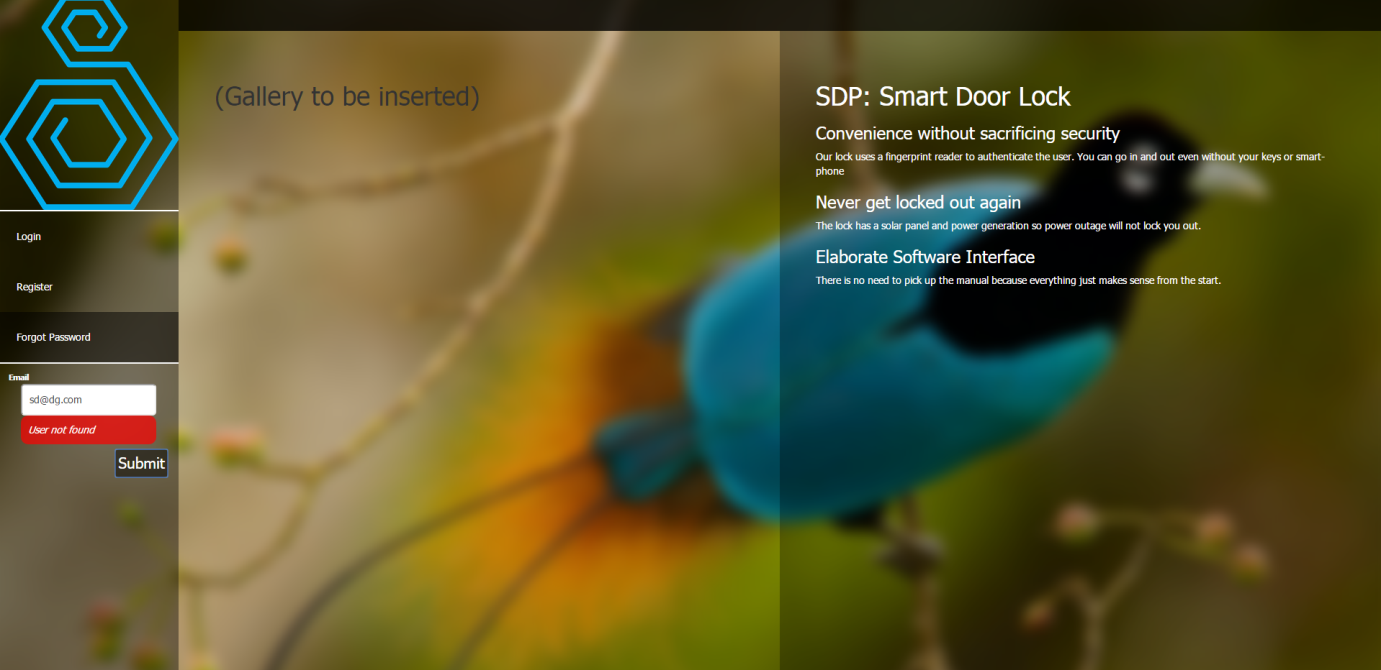
Features

Login Page

User Registration - This is a standard part where the user enter in personal information including name, email, product ID as indicated in the package that will come with the door lock and password. Once this information is confirmed, the user will be redirected to the account page of this web interface.

User Login - Using a registered account with just the email and password, the user will continue to the account page

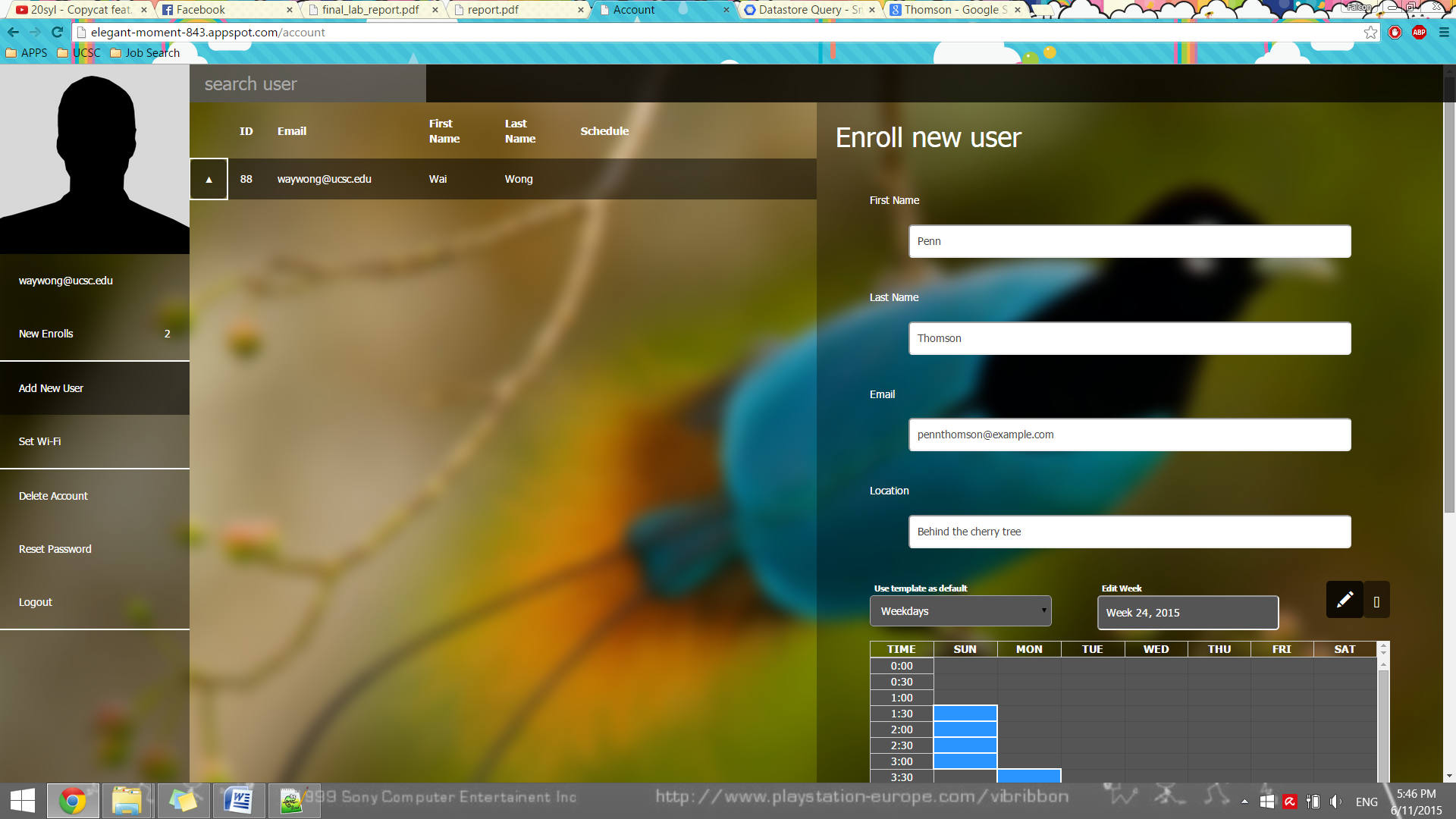
Forgot Password - When the user enters a registered email, an email will be sent or an error will be displayed otherwise as shown below.



Account Page

Push Notifications - When the smart door lock system have new users enrolled on the local interface, notifications will be sent to the internet every thirty minutes. These new additions will be shown on the left hand menu and notify the user to enter names, schedule and email to invite each newly enrolled user to set their password. The physical door lock system has a thirty minute update to synchronize the information between the web server and the physical system. New notifications will be sent via an HTTP post request to the web server during the updates. Setting the Wi-Fi information on the location will trigger this update as mentioned previously.

Add / Edit User - When adding a new user, the current user must provide the name, email, location of the door lock, and the access schedule of this user. After submitting this information, the new user will receive an email invitation with a link to the local interface and under the supervision of an authorized personnel, for the door to be opened, in order to enroll her fingerprint. Editing a user is very similar in that the name, schedule can be changed and even the account can be deleted if the current user has the authorization to do so.

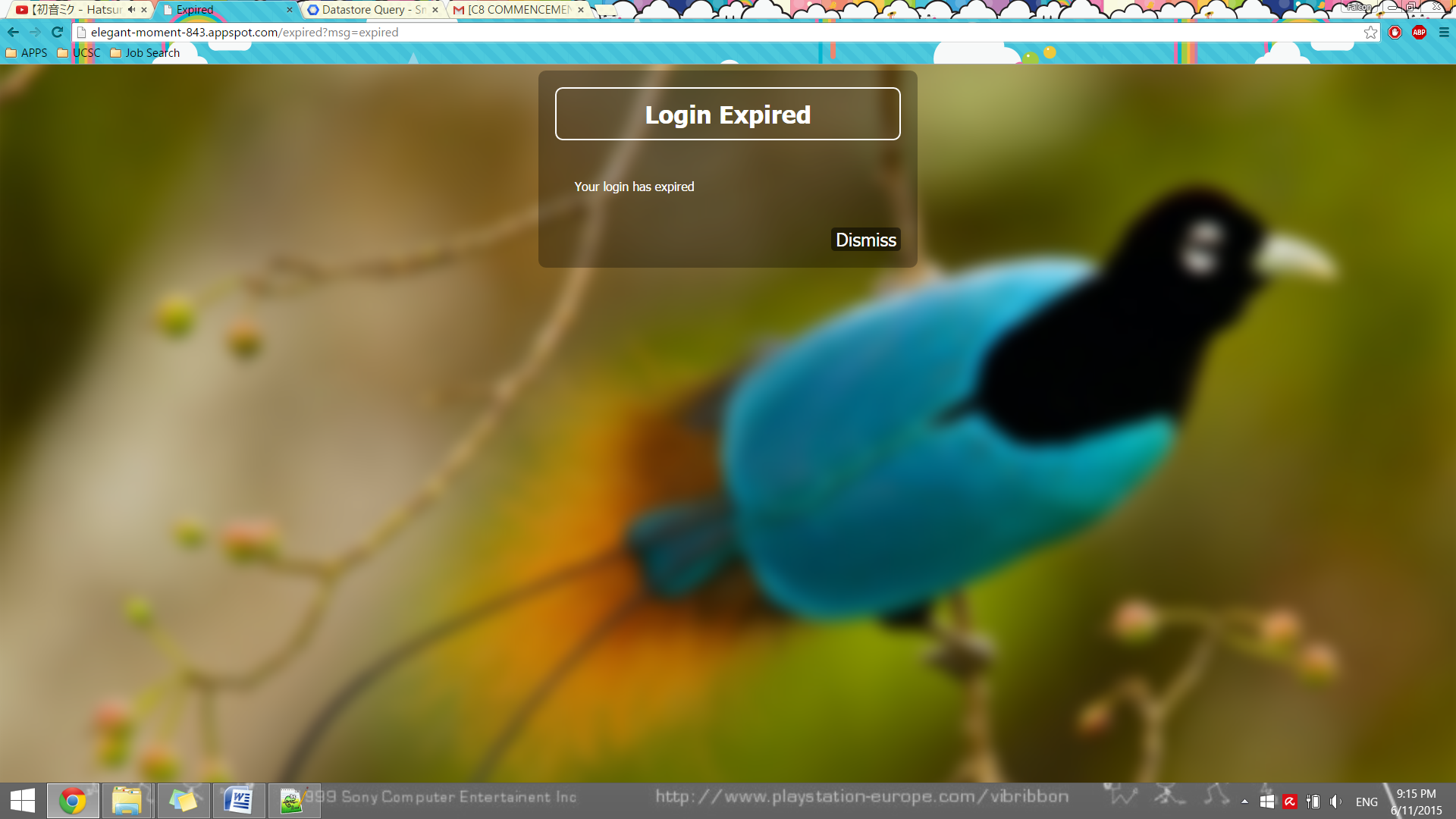


Set Wi-Fi - This information is set in the physical door system such that the system will use the specified network connection to connect to the internet. This includes the correct SSID and password for the connection to work, commonly through a home router. When this information is submitted, the next thirty minute update will

Delete Account - This option is for deleting all information, accounts, and users associated with the door lock including the fingerprint profiles and users on the micro-controller. This will signal the physical system to remove all information during the next thirty minute update.

Reset Password - Completing this form with the correct old user password will reset the user's password.

Login Expired - This page shows that the login session has expired after thirty minutes of no action. For security measures, this also works against the back page button and hacking by manually entering a web URL. In any case, the user is redirected to the login page.



Server Program

Database

The database uses Google's Datastore API and is separated into two parts: the user and the product. The user object is used primarily to store information including first and last names, fingerprint ID, passwords, emails, belonging admin, access schedule, schedule template, SSID, network password, and a generated token which is used for password reset and enrollment invitations. The product object is associated to each door lock which has been manufactured and is used for synchronizing the information for the thirty minute interval update. It includes product ID, changed schedules, deleted users and new users who enrolled through the local door system but has not yet set-up an online account.

None of the functions are very exciting - they simply pull the objects from the database accordingly, set new values and put it back. They also assert the authorization before proceeding and response with error in the case of failure, errors, or denial of access.

Memcache

This is a feature in the Google's cloud server which works the same way cookies do on web browser, except this is for web servers. It stores temporary information and associates each piece of info with a key so the server can use the key to get the information back. This is different than SQL (GQL in this case) in Google's Datastore in that it is a hash table and has no filtering options. The reason for using this is because it is much faster and puts off the load that would otherwise be put on the more expensive SQL manipulations used in the Datastore. Also, memcache has expiry which is perfect for sessions, enrollment expiry and more.

In our case, we used this for forget password in verifying the token which is randomly generated to make sure the user with the link gets to reset the password without knowing her password. The link expires quickly such that even if a curious person looks into her email and click on the link, this person cannot change the password again. The same idea applies to when a person receives email invitation to enroll or receive push notifications. This scheme keeps information more private while not putting any situation into a deadlock.

SMTP

This is Google's emailing API which allows the server to generate and send HTML encoded emails to any recipient from the accounts authorized in the Google accounts which own the server. Put it in a loop and out goes the email to everyone in the list. This is used for forget password, enrollment invitation, and account set-up invitation as discussed previously. To recap: forget password emails a link to reset the password; enrollment invitation directs the person with the certain email to enroll at the physical door system; account set-up invitation links the physically enrolled person with the certain finger ID to set up her online account.

Front End Program

Home Page

As with all other websites, the program uses JQuery to handle mouse events, bind these events to elements and Ajax submit forms to the server. This page checks for errors before sending it off to the web server to minimize the false request attempts in the server. Also, each button is linked to a particular form and depending on the button, the page does not necessarily need to communicate with the server, such as switching between displaying the registration form and the login form.

Account Page

This page is organized the exact same way but handles cookies for expiry as well because this is the page where the user is logged in. Also, this is a single page application such that all server responses will be rendered without refreshing the page. This is done by using JQuery's Ajax method and simply one line to prevent the page from redirecting even after receiving information from the server which is what all browsers do by default.

For visuals such as schedules and list of users, a combination of CSS, JQuery, Glyph Icons is used for resizing, colors, keeping things relative to each other, transparency, fade in / out, hovering, icons, images and texts. The schedule is parsed back and forth to be sent to and from the server and be rendered as HTML elements. The following figure shows most of the visuals.

