Design Report

Team 2

Sean Yap Yu Rong, Lim Ding Heng, Toh Yunqi Cheryl, Sun Shengran

IFS4205 Information Security Capstone Project, AY19/20, Semester 1

September 6, 2019

Overview

This project, **NUSMed**, will be a prototype of a health care system. At this stage, it is not possible to achieve relationships expected within a proper health care system. Therefore, to achieve a meaningful and functional health care system, the envisioned health care system is designed to be condensed and compact, with core and essential functionalities. The system is streamlined to achieve the best user experience without neglecting core functionalities.

To give a summary, the envisioned system will rely on trusted administrators to perform registration of users, such as patients, therapists and researchers. After registration, therapists will be able to request permissions from patients to perform his medical duties. Permission requests include two subsets, either account or record permission. It will be assumed that account permissions are necessary for any therapist to access records. More information about permissions will be discussed in more details below.

Similarly to permissions, there is also a system for diagnosis. As explained above, it is not possible to produce a fully encompassing system such that patients have treatments and treatments are performed by doctors. However, we find that it is absolutely necessary in a health care system for therapists to view and set a patient's diagnosis; as such, there is a also functionality for diagnosis to be attributed to a patient to show some illness inflicted him or her for some time period. This is important for therapists to assess as patients' current illnesses are dependent on previous diagnosis. Records can be attributed to multiple diagnosis to show which records are relevant for treating which illness.

There are two databases, one "main" database and one "logging" database. The "main" database performs typical operations related to the system while the "logging" database facilitates the storing of application logs. The "logging" database will also be used to backup transactional and or query logs of the "main" database. This is shown in more detail in the Enhanced Entity Relationship (EER) diagram, located on the next page.

All pages served by the web server and all communication will be served over Transport Layer Security 1.3 (TLS1.3). TLS provides authentication of the server to the client as well as integrity of the transmitted data since it prevents attackers from modifying the content in transit. Using TLS also prevents replay attacks; a captured stream of TLS data is prevented from being replayed at a later time.

The following 3 diagrams are shown below to aid visualisation of the envisioned system. However, for more information on the infrastructure or database design, please refer to the tools and assessment report and database design report. Instead, this report will focus on system design from the user's perspective.

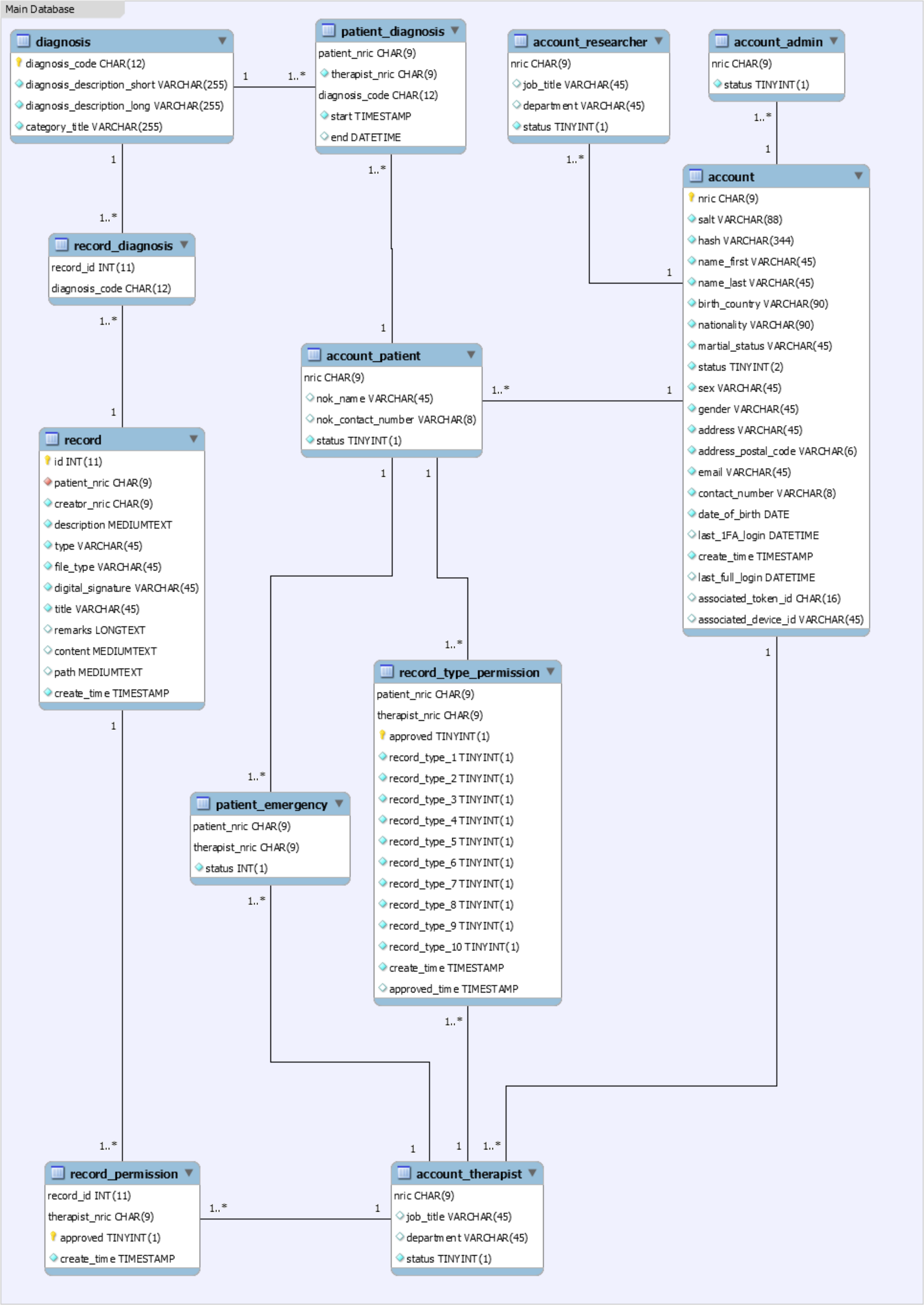
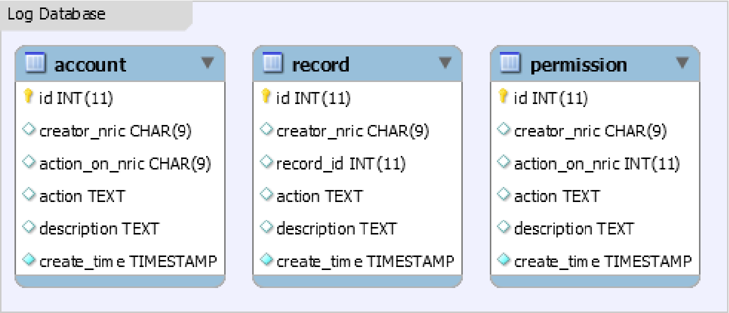


Figure 1: Enhanced Entity Relationship (EER) diagram of the "main" database



Log Database

account
- id INT(11)
- creator_nric CHAR(9)
- action_on_nric CHAR(9)
- action TEXT
- description TEXT
- create_time TIMESTAMP

record
- id INT(11)
- creator_nric CHAR(9)
- record_id INT(11)
- action TEXT
- description TEXT
- create_time TIMESTAMP

permission
- id INT(11)
- creator_nric CHAR(9)
- action_on_nric INT(11)
- action TEXT
- description TEXT
- create_time TIMESTAMP

Figure 2: Enhanced Entity Relationship (EER) diagram of the “log” database

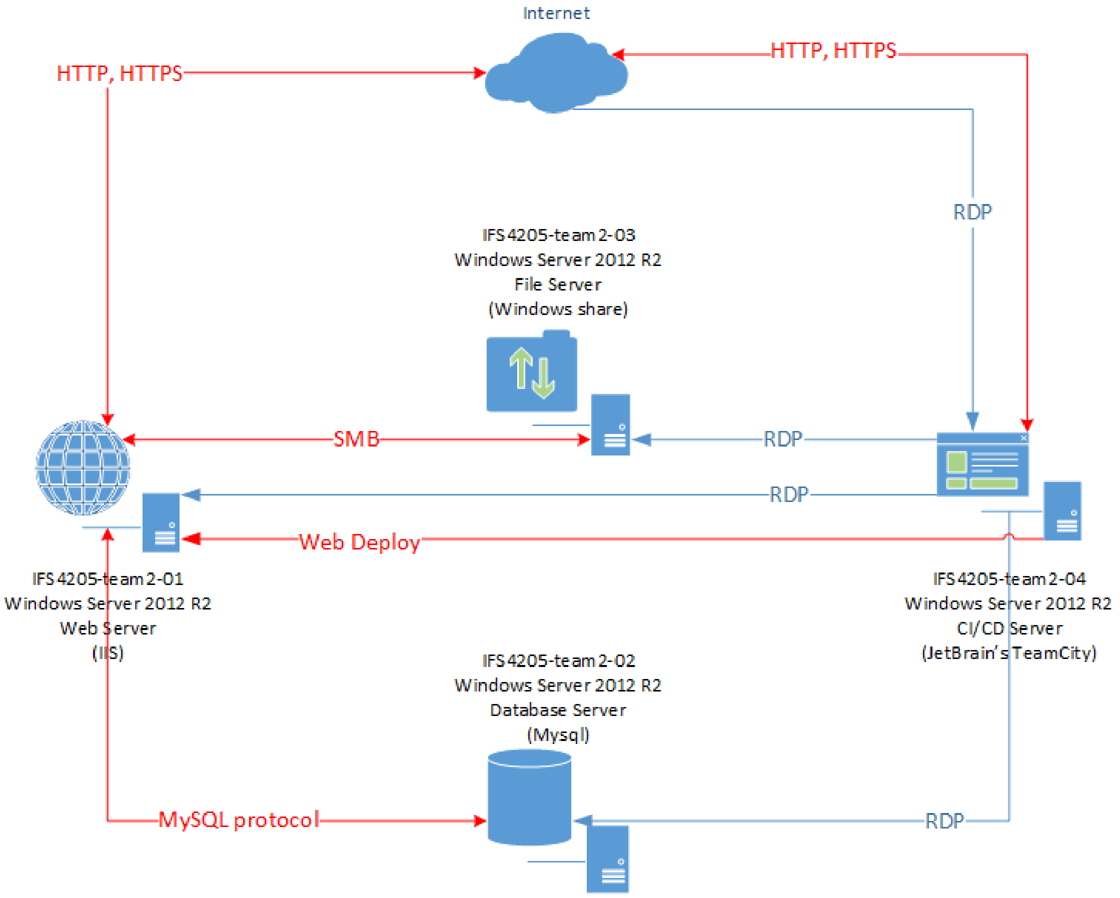


Figure 3: Architecture Diagram of entire system

1 Subsystem 1 (Multi-Factor Authentication)

1.1 Overview

The multi-factor authentication subsystem will involve what the user knows (password) and what the user has (smartphone & NFC tag). As mentioned in the Tools Assessment Report, the NFC tag is a factor in this multi-factor authentication subsystem so that it can also facilitate the requirement of validating a data entry of a comatose patient. Using NFC tags would address the ease-of-use concern without neglecting the authentication strength.

1.2 Claims and Assumptions

- The administrator refers to a clerk, receptionist or nurse; he or she is the most trustworthy individual.
- Due to the first item above, the administrator will always be responsible for user registration, including the assigning of tokens.
- Every stakeholder owns an Android base smartphone with an in-built NFC reader and, hence, will be able to utilise the services this health care system provides.

1.3 Tools and Software

- Android phones (at least version 4.0.3) with in-built NFC reader
- NFC tag

1.4 Implementation

1.4.1 User Registration

1. User approaches an administrator to register for an account. This mirrors the common procedure in Singapore whereby a patient first registers him or herself at the registration counter; or perhaps the induction of a new employee, therapist or researcher.
   (a) Administrator logs in to the NUSMed web app, selects the administrator role, and navigates to the registration page.

   (b) Administrator refers to the user to key in his details including his NRIC and password.

   (c) Administrator selects the roles for the user and submits the form.

   (d) The web app will utilize the key derivation function, Password-Based Key Derivation Function 2 (PBKDF2), to generate a 256 bytes hash from the password. PBKDF2 works by taking in the password and a salt generated by a secure random number generator (RNGCryptoServiceProvider), passing them through a pseudo-random function based on HMAC-SHA512, and iterate 10 000 times to generate the final 256 bytes hashed password.

   (e) Both the hashed password and salt will be stored into the database.
2. Administrator will issue a NFC tag with a unique ID to the user.
   (a) The unique ID is of 16 bytes and will be generated and written to the NFC tag by the tag's manufacturer.

   (b) The unique ID is a random UUID which can be generated by Java's UUID class.

   (c) The administrator will read the unique ID, and associate it with a user by saving it with the database entry of the user.
3. User will install NUSMed's mobile app.
   (a) Upon running the mobile app, a device ID of 16 bytes will be generated the same way as in step 2(b).

   (b) The device ID will be stored in the mobile app's encrypted shared preferences (EncryptedSharedPreferences) and the encryption algorithm is AES-256 GCM. The encryption key would be stored securely in Android's keystore.

4. User will log onto the mobile app with the same NRIC and password he provided to the web app.
    (a) The login request from the phone to the web service will be secured by TLS1.3.
    (b) The user is allowed to proceed with the next step only if the web service responds that the user is validated successfully.
5. User will scan the issued NFC tag from the mobile app.
    (a) The unique ID of the NFC tag together with the device ID will be sent to the web service.
    (b) The web service ensures the NFC tag's unique ID matches the saved unique ID of the associated user. It also ensures the device ID is unique in the database before storing it into the associated user's entry.
    (c) If successful, the user will remain permanently logged in on the mobile app.
6. The registration process is now complete.

1.4.2 User Login

1. User logs in on the web app with his NRIC and password (1st authentication factor)
    (a) Web app will request for the user's associated salt from the database.
    (b) Web app will utilize PBKDF2, with the parameters being the user's associated salt, and the password given in step 1, to generate a hash of 256 bytes.
    (c) Web app will validate if the generated hash matches the user's associated hashed password in the database.
    (d) User will be able to proceed onto the next step if the validation is successful.
2. Web app directs to another page with a prompt for the user to scan his issued NFC tag with the NUSMed's mobile app (2nd authentication factor)
    (a) Web app polls the application cache for a specific user variable every second for 30 seconds to check if the user has scanned his issued NFC tag within 30 seconds from the time he was prompted. If the cache has already been filled, it would mean that the process has not been followed in order and could have been fraudulent, this process would then end here.
    (b) User will scan his NFC tag with the mobile app.
    (c) The unique ID of the NFC tag together with the device ID retrieved from the application's encrypted shared preferences will be sent to the web service.
    (d) The web service ensures the NFC tag's unique ID and device ID belong to the associated user.
    (e) If it matches, the web service will update the variable in the cache which would be checked by the polling as in step 2(a).
3. The user is now authenticated and will be able to select from his/her registered roles for the current session.

1.4.3 Authenticating the Upload of Data for an Emergency Patient

For an emergency patient, he/she would be unable to create/upload any records personally or accept requests from therapists to view/create/upload his/her records. Hence, a therapist has to do so on behalf of the patient.

As such, it is necessary to authenticate the identity of the therapist who is doing so on behalf of the patient, as well as the identity of the patient. The following steps will detail this authentication process.

1. An emergency patient is admitted and an administrator would assign an appropriate and available therapist to the patient through the administrator portal.
2. The assigned therapist would have permission to view/create/upload any record for the emergency patient.
3. To view/create/upload records for the patient, the therapist would be required to use his/her smartphone with NUSMed's mobile app to scan the NFC tag of the patient. This verifies the identity of both the therapist as well as the patient.
4. This access will be revoked once the treatment is over or the patient recovers and sets the permission manually.

1.4.4 Mobile Interface

As mentioned in the user registration process, when a user first installs and runs the app, the user will be presented with a login page. The user will then key in the same credentials used when registering an account for the web app. Upon validating the credentials, the "Scan NFC" page will be shown and the user is required to scan the NFC tag issued to him/her. The registration process will be complete only after validating the issued NFC tag. The user is now permanently logged in on the mobile app. The user will then be directed to the "Select Role" page to select his/her role from the roles registered for him/her by the administrator. Finally, the user will be directed to the "Home" page where different buttons would be available depending on the current role selected. There would be a "Change Role" button to direct the user to the "Select Role" page for both patients and therapists.

As a patient, there would be an "Upload Record" button to direct the user to the "Upload Record" page where he/she would be able to upload records of different types.

As a therapist, there would be 3 buttons: "Upload Record (for Patient)", "Upload Record (for Emergency Patient)", and "Scan NFC (for Emergency Patient)". The "Upload Record (for Patient)" page is meant for the therapist to upload a record for a conscious patient. In the scenario where the patient is unconscious or is in an emergency state, the therapist would use the "Upload Record (for Emergency Patient)" or "Scan NFC (for Emergency Patient)" buttons to upload records on behalf of the patient. The "Upload Record (for Emergency Patient)" button allows the therapist to upload a record from his/her mobile app for the emergency patient. The "Scan NFC (for Emergency Patient)" button is used when the therapist uploads a record from the web app and the therapist is required to scan the NFC tag of the emergency patient to authenticate the identity of the patient.

1.5 Security Considerations

By using TLS1.3, the authentication of the web server to the client is provided. TLS1.3 protects the confidentiality and integrity of any data in transit between the web server and client. Thus, an attacker will not be able to sniff the password during transmission. It also prevents a captured stream of TLS data from being replayed at a later time as seen in replay attacks.

For data at rest, such as unique IDs and passwords, encryption or hash functions are employed to protect the confidentiality and integrity of the data. The device ID generated for NUSMed's mobile app is stored in the encrypted shared preferences so as to prevent other mobile applications from being able to retrieve or tamper with the generated device ID. The user's password is hashed by utilizing PBKDF2 which is slow by design so as to mitigate the risk of successful brute force attacks on the hashed password.

2 Subsystem 2 (Admins, Therapists and Patients Functionalities)

2.1 Overview

This subsystem includes several components to drive the core system of NUSMed. There are many components to this subsystem, mainly, the web app, web services and database.

2.2 Claims and Assumptions

Claims for this subsystem will be split separately according to systems.

Accounts and Roles:

- A single user or account will be able to possess multiple roles at the same time. However, users may only perform the functionality of a single role at a time.
- Administrators are unable to perform administrative actions on themselves. They require another administrator to perform actions on their account.
- There is no business need for concurrent logins for any user. As such, it is not possible for a single user to log in to the system on two separate browsers or machines.
- While all roles are able to edit their own contact information, other sets of data is restricted, similar to Singapore's medical system. Patients are able to edit their next-of-kin information and no one else would be able to do so, including administrators. Therapists and researchers are unable to edit their job title and department but administrators are able to.

(Medical) Records:

- Therapists innately requires patient's details to proceed with treatment of any kind. The justification here is that the patient's details are crucial to medical diagnosis and treatment. Hence, requests for record permissions will innately request for permission to view patient information.
- Records will always belong to patients even when created by therapists.
- Therapists need not have a record store; records cannot be uploaded or saved into the system without attributing or assigning it to a patient; specifically by therapists.
- Patient personal and record information may only be viewed by therapists if granted permissions by and only by the specific patient.
- Patients are able to remove a subset of permissions but not "hide" records from therapists. For instance, if a therapist has full access to a patient except a single record, the record will be redacted except its name and date of creation. This is important as therapists needs to know if some information has been omitted to perform medical duties.
- Records are categorised according to "record types" and are used as groupings for access control.
- Records may have remarks that may be editable by therapists but un-editable to patients. Note that more concrete and official information should be created as a "Medical Note" instead. This follows the medical practice in Singapore.
- Records can either be plain text content or be a file such as an image, movie or document. This determination will be as according to record type.
- Record types are one of these ten types:
  1. Medical Note

2. Height Measurement
3. Weight Measurement
4. Temperature Reading
5. Blood pressure Reading
6. ECG Reading
7. MRI
8. X-ray
9. Gait

(Medical) Diagnosis:

- Patients can be attributed a diagnosis. This will serve as treatment history in the system. The history of therapists that assign the diagnosis will be recorded.
- Diagnosis can also be tagged to records to show the relevance of records that will prove useful to determine treatment and or diagnosis history.

2.3 Tools and Software

This section has been covered in detail in the Tools Assessment Report. As such, only client side frameworks and security related and related to the interface will be shown here. These frameworks were not disclosed in the earlier report.

Client-side Frameworks:

- JQuery v3.4.1
- Twitter Bootstrap v4.3.1: front-end framework for web development and design
- Font Awesome: font-end framework for icons
- Toastr v2.1.4: JavaScript library for non-blocking notifications

Security Related Frameworks:

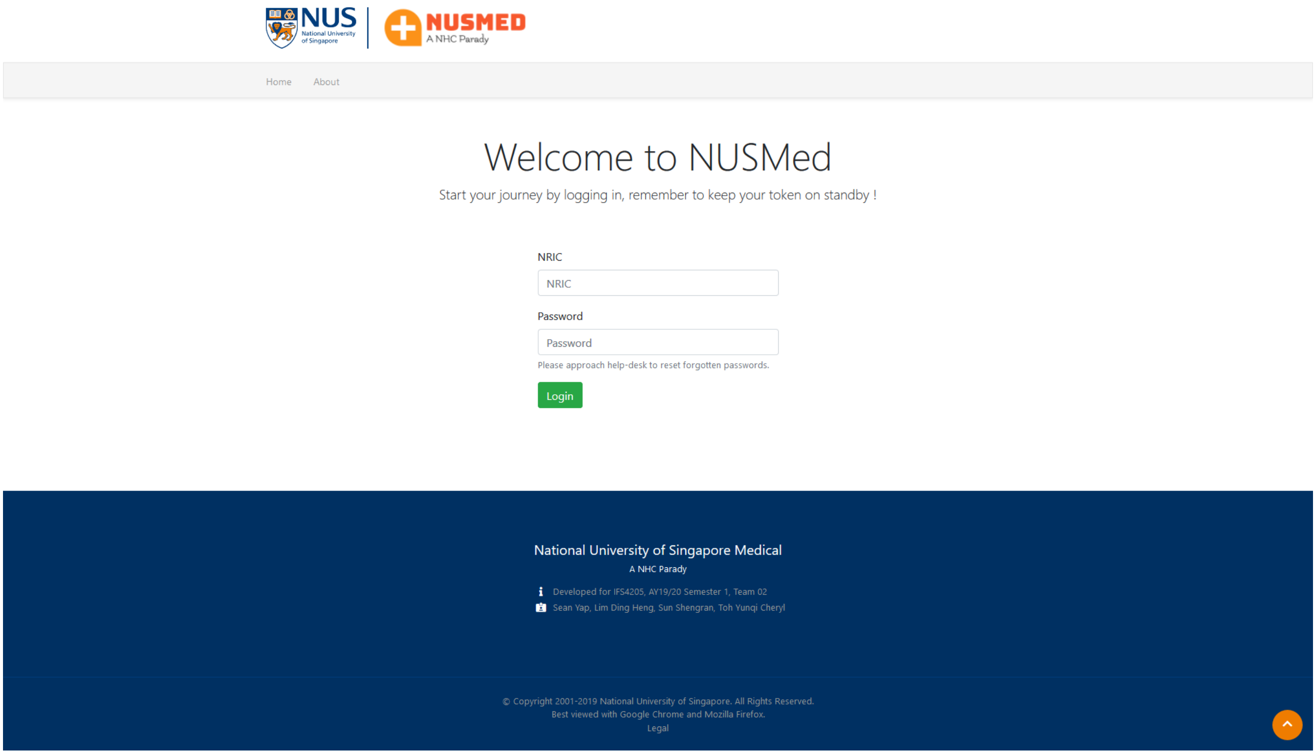
- BouncyCastle v1.8.5: Collection of cryptography APIs for encryption; used for encryption of session data, hashing of passwords, encryption cache values and etc.
- HTMLSanitizer v4.0.217: Cleans HTML from constructs to prevent cross site scripting (XSS)
- NWebsec v5.1.1: Security library to configure security headers, detect re-directions and control cache headers.

2.4 Implementation

2.4.1 Interface for Authentication

The login page will reside on the home page of the web app. The form on the page will be utilising Ajax calls to facilitate the login process. Upon successful authentication using username and password, a modal, "popup", will be invoked to carry on the authentication process as detailed above. The modal will show users a countdown timer and a cancel button.

A screenshot of the Login page is provided below to aid visualisation. The modal popup is not shown.



Welcome to NUSMed

Start your journey by logging in, remember to keep your token on standby !

Please approach help-desk to reset forgotten passwords.

National University of Singapore Medical

A NHC Parady

Developed for IFS4205, AY19/20 Semester 1, Team 02

Sean Yap, Lim Ding Heng, Sun Shengran, Toh Yunqi Cheryl

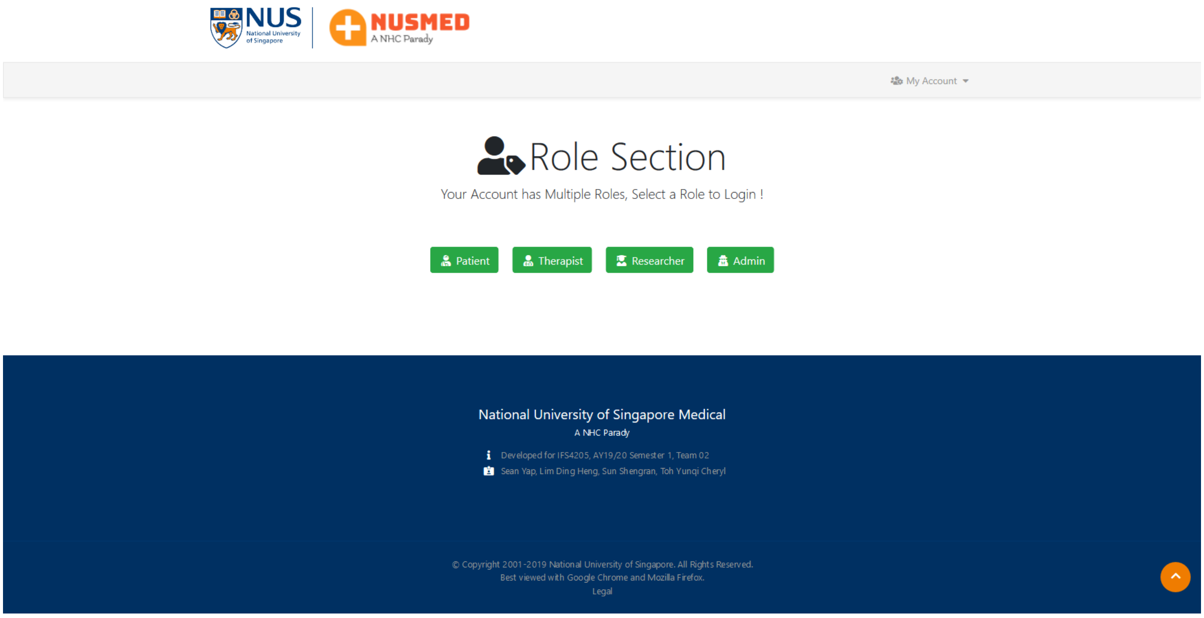
© Copyright 2001-2019 National University of Singapore. All Rights Reserved.
Best viewed with Google Chrome and Mozilla Firefox.
Legal

Figure 4: Interface for Login page

2.4.2 Interface for Role Selection

Upon login, if an account possess multiple roles that are "active", they will be redirected to the Role Selection page. The role the web app assigns to the user, upon login, would be called "Multiple" instead of any role. To be specific, the ticket encrypted in the cookie would have that role instead of the other real and proper roles. This ensures that the user is unable to access any pages or functionalities except to visit this Role Selection page to select another role.

A screenshot of the Role Selection page is provided below to aid visualisation. In this case, the authenticated user possess multiple and all roles that are also active; hence, the user is able to see and select any role. In the event that a user do not possess a role, the button will be omitted from the page via server-side upon page load. This is important to not disclose certain information which will be discussed in the Security Considerations section below.



Role Section

Your Account has Multiple Roles, Select a Role to Login !

National University of Singapore Medical
A NHC Parady

Developed for IFS4205, AY19/20 Semester 1, Team 02
Sean Yap, Lim Ding Heng, Sun Shengran, Toh Yunqi Cheryl

© Copyright 2001-2019 National University of Singapore. All Rights Reserved.
Best viewed with Google Chrome and Mozilla Firefox.
Legal

Figure 5: Interface for Role Selection page

In the event that a user, such as patients, only possess one single role, this whole process will be omitted and the user will be able to obtain the correct role straight away without interruption.

In both cases, upon obtaining a proper role, the user will be assigned a proper ticket with the selected role that will be encrypted in a cookie and will be redirected to the dashboards of the specific role.

2.4.3 Interface for All Authenticated Users

All authenticated users share the same interface but with restricted access to directories and pages.

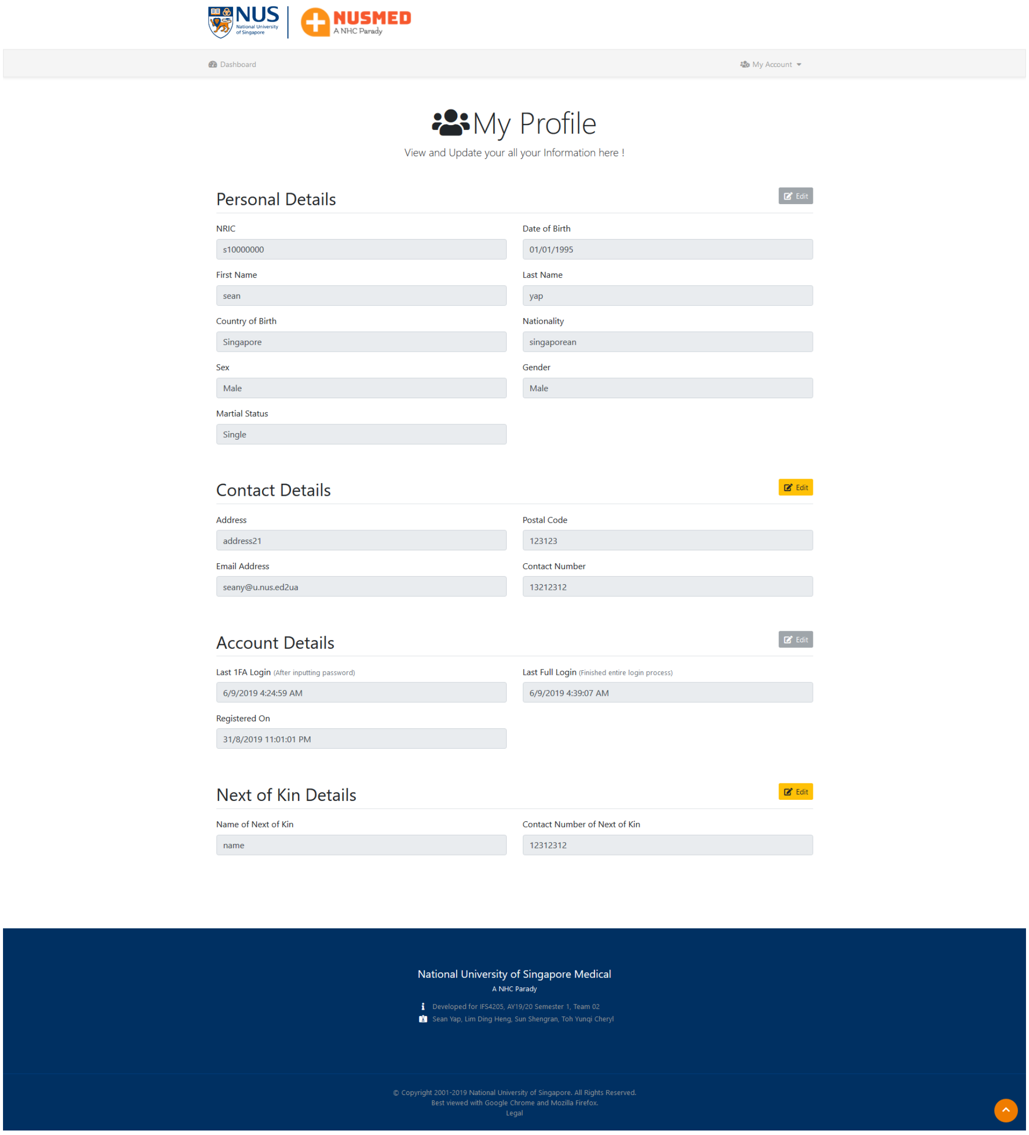
1. My Account

   All authenticated users with proper roles will be able to view the “My Account” drop-down which displays pages with functionalities related to account information and authentication.

   (a) My Profile

   This page allows users to view and edit, certain, information related to them, including their personal information, contact information and etc. Here, patients will also additionally able to edit his or her next-of-kin information while therapists and researchers will be able to edit his or her job information. Fields not related to the selected role at the moment of time will not be shown to the user.

   The screenshot below shows a patient’s view of his profile page.



My Profile

View and Update your all your Information here !

Personal Details

NRIC: s10000000	Date of Birth: 01/01/1995
First Name: sean	Last Name: yap
Country of Birth: Singapore	Nationality: singaporean
Sex: Male	Gender: Male
Martial Status: Single	

Contact Details

Address: address21	Postal Code: 123123
Email Address: seany@u.nus.ed2ua	Contact Number: 13212312

Account Details

Last 1FA Login (After inputting password): 6/9/2019 4:24:59 AM	Last Full Login (Finished entire login process): 6/9/2019 4:39:07 AM
Registered On: 31/8/2019 11:01:01 PM	

Next of Kin Details

Name of Next of Kin: name	Contact Number of Next of Kin: 12312312

National University of Singapore Medical
A NHC Parady
Developed for IFS4205, AY19/20 Semester 1, Team 02
Sean Yap, Lim Ding Heng, Sun Shengran, Toh Yunqi Cheryl

© Copyright 2001-2019 National University of Singapore. All Rights Reserved.
Best viewed with Google Chrome and Mozilla Firefox.
Legal

Figure 6: Interface for Profile page

(b) Change Password

This page allows users to change their password. Password generation follows the login and registration process of password security, checking and storing.

(c) Switch Role

"Switch Role" is not a web page but a button that allows users to return to the role selection page to select another role instead of going through the entire process of logout and login simply to switch roles.

(d) Logout

"Logout" is not a web page but another button that simply signs the user out via removing the form authentication ticket and updating database values to indicate user logout.

In the event of concurrent logins, the older session will be kicked out and redirected to the home page with a popup shown.

In the event of session timeout, a popup will be shown on the page that the user is on to show that the session has been terminated; including the removal of existing authentication tickets and the whole logout process. Additionally, one minute before session timeout, another popup will be shown to warn the user.

2.4.4 Interface for Patients

Patients will have access to these pages:

- Dashboard

  Upon login, patients will first be presented with a dashboard showing statistics such as how many therapists have access to his information, number of records and etc. Most importantly, his past and present diagnosis will be presented in a timeline view. Lastly, important notifications will be presented here such as in the event for therapists requesting for permissions.

- My Therapists

  Patients will be able to visit this page to view a list of therapists. Both therapists that have been granted or are requesting permissions will be shown in a list format. The listing here will be sorted in descending order by the date and time of which the permissions has been requested for.

  Here, many actions can be performed such as changing permissions of therapists whether be it removal of all permissions, granting all permissions, restricting permissions to certain type of records or by individual records. Additionally, there will also be a button to view the therapist's non-sensitive information; such as first name, last name, job title and department he or she belongs to.

  If permissions have not been granted, the normal therapist item will not be shown but, instead, replaced with a different item that shows the requested permission, specifically by means of record type or all permissions, and a button that allows the patient to grant the requested permission.

  All these actions will be performed via Ajax and will not feature any full page loads. It will be more akin to a web app than a web site. All of these actions will also restrict patients to a world view without knowledge of other patients or therapists. He or she will be unable to grant therapists of permissions unless requested for and will not be able to view any other therapists.

- My Records

  - View

    This page will display all of the patient's records (records that he or she owns) in a table format; this includes information such as title, record type, date of creation, person who created record and description. Patients will only have read access to their records and will not be allowed to edit nor delete records.

    However, patients will be able to download or view records in the browser. Text, images and movies will be supported for viewing in the browser via HTML 5 player that is inbuilt into modern browsers and will be displayed to the patient via modal popup.

  - Upload New Record

    This page will be solely for patients to upload records, showing simply a form. This form will be dynamically altered via Ajax depending on the record type chosen. This is because, as stated above, certain record types only requires text content while others requires a file to act as the record and thus be uploaded. For instance, if the record type chosen is of type "Temperature Reading", the form will be altered to display a multi-line textbox instead of upload file control.

2.4.5 Interface for Therapists

Therapists will have access to these pages:

- Dashboard

  Upon login, therapists will first be presented with a dashboard showing statistics such as the number of patients he currently has permissions to and the number of patients that has not granted him or her permissions. To facilitate usability, instructions on how the system words with regards to permissions and record handling will be displayed on this page along with links to other pages that therapists have access to.

- My Patients

  – View

    This page serves all functionalities related to a therapist's patients. There are a few subsets of functionalities here that can be seen in 3 groupings.

    Firstly, this page will allow therapists to view his or her patients. Both patients that have granted or pending will be shown in a list format. The listing here will be sorted in descending order by the date and time of which the permissions has been requested for. Here, there will be several buttons on each row and patient, each performing a functionality. One button will be able to perform permission related functions such as requesting a new set of permissions, via a collection of record types, or remove the patient permission completely (akin to treatment has ended). There will also be a button to view the patient's private information; such as personal, contact and next of kin information. Additionally, there will be a button for therapists to view patients records. This will be further explained below.

    If permissions have not been granted, the normal patient item will not be shown but, instead, replaced with a different item that shows the requested permission, specifically by means of record type or all permissions, and a button that allows the therapist to retract the request.

    Secondly, the functionality of emergency patients is also provided here. After the therapist has been granted MFA "override", for the lack of a better term via an admin, will be highlighted and display a different color. There will also be instructions provided for the therapist to perform the correct actions to invoke the granting of access to the patient. For example, "Use your registered device to scan the patient's token".

    Lastly, via the list of patients, records can be viewed through selecting the "view records" button which will trigger a collapse panel to un-collapse. At this stage, the web app retrieves and updates the underlying hidden panel, populating it with entries that would be the selected patient's records. Each record can then be interacted with in similar methods as with the patient's list. This includes information such as title, record type, date of creation, person who created record and description. Therapists will only have read access to the records and will not be allowed to edit nor delete records. Text, images and movies will be supported for viewing in the browser via HTML 5 player that is inbuilt into modern browsers and will be displayed to the patient via modal popup.

    All these actions will be performed via Ajax and will not feature any full page loads. This allows for the page to contain several functionalities.

  – Submit New Request

    This page provides therapists with the functionality of requesting for permissions from a patient that is, perhaps, not under his care. For instance a newly registered patient first meets his therapist. In this page, the therapists is allowed to only search through a list of all the patients via NRIC to identify the patient of interest and select "request". Using only NRIC and not first nor last name would prevent therapists from searching for others other than the patients he or she comes into contact with.

A modal popup will once again be used to allow the therapist to select what record types he would like to request permissions for and select “submit”, to submit the request.

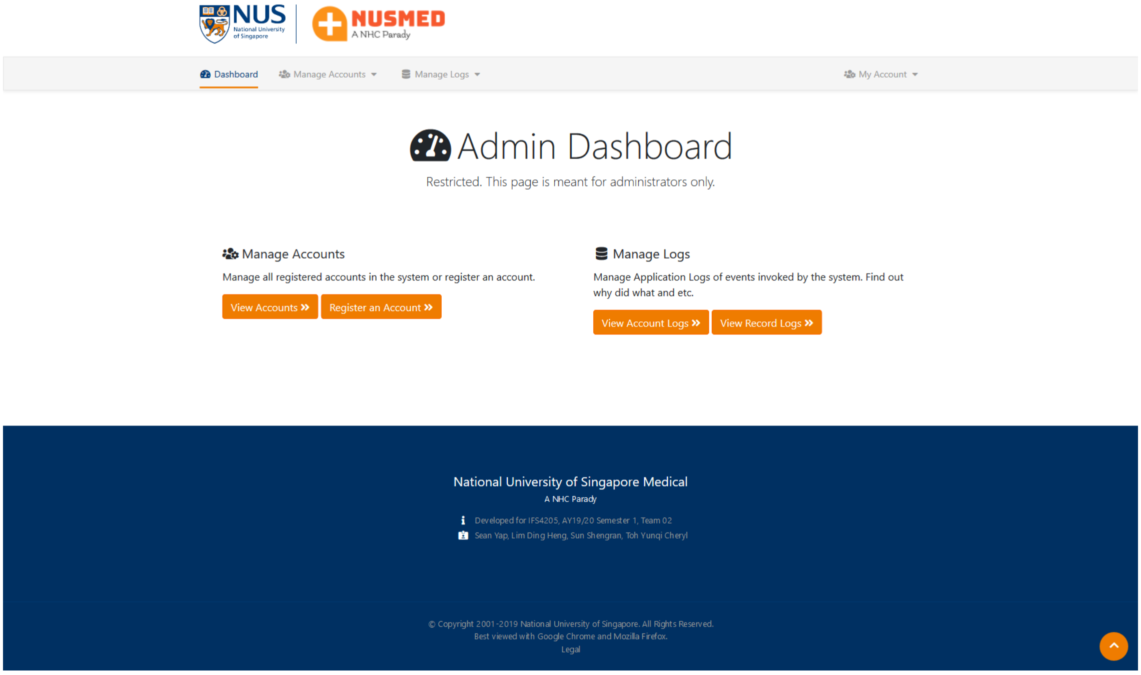
2.4.6 Interface for Administrators

Administrators will have access to these pages:

- Dashboard

  Upon login, administrators will first be presented with a dashboard showing the functionalities he or she has access to.

  Draft interface of the dashboard is shown below.



Admin Dashboard

Restricted. This page is meant for administrators only.

Manage Accounts

Manage all registered accounts in the system or register an account.

Manage Logs

Manage Application Logs of events invoked by the system. Find out why did what and etc.

National University of Singapore Medical

A NHC Parady

Developed for IFS4205, AY19/20 Semester 1, Team 02

Sean Yap, Lim Ding Heng, Sun Shengran, Toh Yunqi Cheryl

© Copyright 2001-2019 National University of Singapore. All Rights Reserved.
Best viewed with Google Chrome and Mozilla Firefox.
Legal

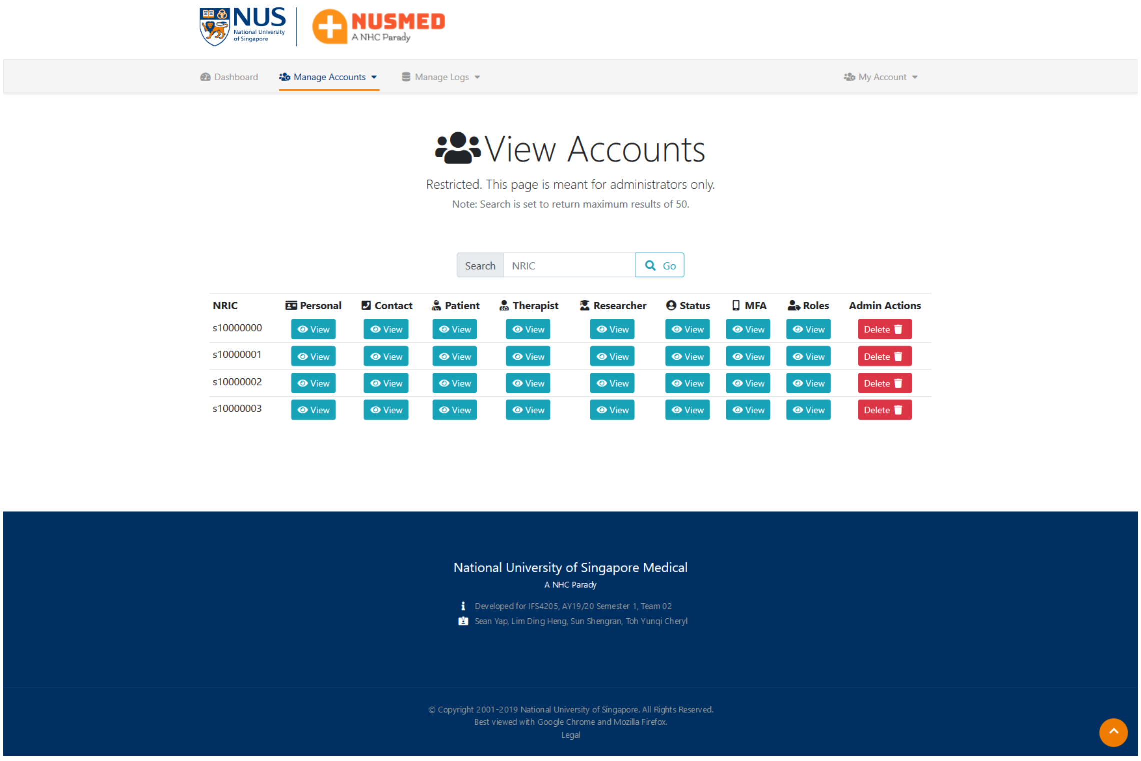
Figure 7: Interface for Login page

- Manage Accounts
  - View Accounts

    This page will provide administrators the ability to view and manage all accounts. First, on this page, administrators will be able to perform crucial actions such as changing the status of roles, changing the account status, changing MFA token IDs (but unable to view) and changing staff (therapists and researchers) information of accounts. All account information may be viewed by the administrators. However, personal, contact and next-of-kin information can only be edited by the account holder; administrators will be prevented from editing these information to prevent misuse.

    To ensure data privacy, administrators are unable to search the list of accounts in any other methods except via NRIC. All information about the accounts that returns in a search will also be displayed in a format that hides all information except the NRIC. Administrators need to choose and click buttons specific to certain functionalities to trigger the modal popup to display the specific user interface relevant for those actions. This prevents simple incidents such as patients shoulder-surfing administrators such as clerks working at their desks.

In the screenshot below, it is evident that no one would be able to retrieve any information about any account as all fields are hidden within other modals. Any action such as viewing of personal data of an account, will be logged. This restricted style of user interface ensures that administrators will be deterred from abusing their authority.



View Accounts

Restricted. This page is meant for administrators only.

Note: Search is set to return maximum results of 50.

Search NRIC Go

NRIC	Personal	Contact	Patient	Therapist	Researcher	Status	MFA	Roles	Admin Actions
s10000000	View	View	View	View	View	View	View	View	Delete
s10000001	View	View	View	View	View	View	View	View	Delete
s10000002	View	View	View	View	View	View	View	View	Delete
s10000003	View	View	View	View	View	View	View	View	Delete

National University of Singapore Medical

A NHC Parady

Developed for IFS4205, AY19/20 Semester 1, Team 02

Sean Yap, Lim Ding Heng, Sun Shengran, Toh Yunqi Cheryl

© Copyright 2001-2019 National University of Singapore. All Rights Reserved.

Best viewed with Google Chrome and Mozilla Firefox.

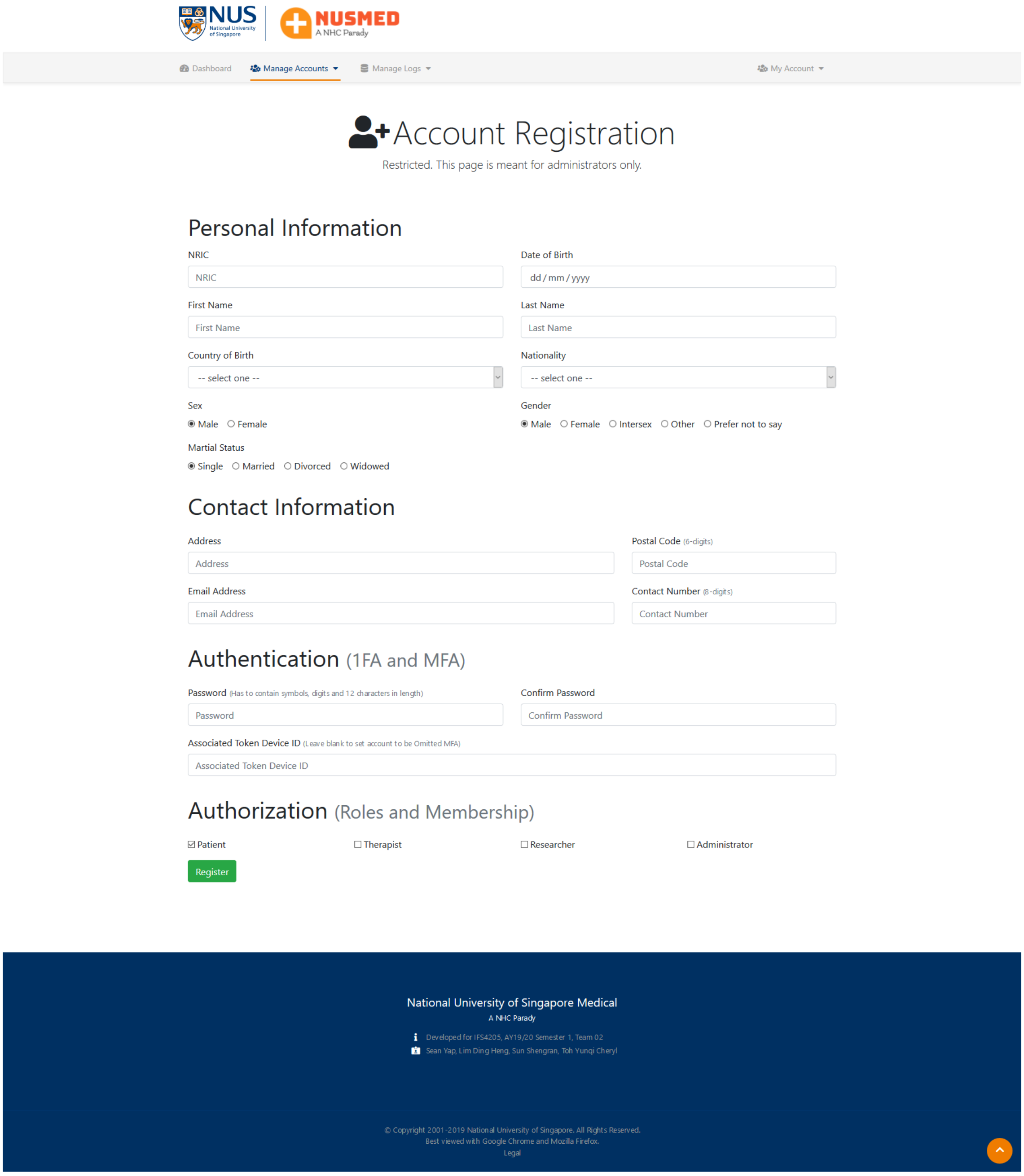
Legal

Figure 8: Interface for administrator view accounts page

- Register Account

  This page as stated in subsystem 1 facilitates the registration of a user. Administrators will be filling in this form except for the password fields. Similar to some services in Singapore, such as hotels, the administrators could also register a temporary password and oversee the patient in changing his or her password. In both cases, the administrator will oversee the entire registration process.

  Screenshot of the registration page is shown below.



Account Registration

Restricted. This page is meant for administrators only.

Personal Information

NRIC: NRIC

Date of Birth: dd / mm / yyyy

First Name: First Name

Last Name: Last Name

Country of Birth: -- select one --

Nationality: -- select one --

Sex: ● Male ○ Female

Gender: ● Male ○ Female ○ Intersex ○ Other ○ Prefer not to say

Martial Status: ● Single ○ Married ○ Divorced ○ Widowed

Contact Information

Address: Address

Postal Code (6-digits): Postal Code

Email Address: Email Address

Contact Number (8-digits): Contact Number

Authentication (1FA and MFA)

Password (Has to contain symbols, digits and 12 characters in length): Password

Confirm Password: Confirm Password

Associated Token Device ID (Leave blank to set account to be Omitted MFA): Associated Token Device ID

Authorization (Roles and Membership)

☑ Patient ☐ Therapist ☐ Researcher ☐ Administrator

National University of Singapore Medical
A NHC Parady
Developed for IFS4205, AY19/20 Semester 1, Team 02
Sean Yap, Lim Ding Heng, Sun Shengran, Toh Yunqi Cheryl

© Copyright 2001-2019 National University of Singapore. All Rights Reserved.
Best viewed with Google Chrome and Mozilla Firefox.
Legal

Figure 9: Interface for administrator register account page

- Manage Logs

  The following three pages will display a table displaying logs ordered in descending order by date and time. Administrators are able to filter the table by NRIC of action perpetrator, NRIC of action taken on, date, and action type. Each type of logs are segregated into three pages to allow for easy viewing of logs.

  - Account Logs
  - Records Logs
  - Permission Logs

2.5 Security Considerations

- Using HTTPS utilizing TLS1.3 to ensure confidentiality and integrity from and to the web-server, android app and user's web browser.
- Disallowing all file extensions except specially selected file extensions, dependent on the record type to be uploaded in to the file server.
- Parameterizing all SQL queries to prevent SQL injections of all forms.
- Prevent cross site scripting (XSS) by sanitizing all inputs and outputs. Additionally, placing outputs from database into HTML controls that do not permit browser execution to add on an additional layer of mitigation in event of issues with sanitization. For instance, placing outputs into disabled text-boxes when possible instead of plain text.
- Utilizing application cache to detect and prevent concurrent login sessions.
- Using viewstate variables and web objects placed on the page to prevent Cross-Site Request Forgery (CSRF).
- Utilizing application cache to detect and prevent concurrent login sessions.
- Authentication on every request via form authentication and form ticket to enforce role based access control to determine access on the directory level.
- Prevent user error in programming that leak information via error codes, debug information and status messages through the use of custom error pages that are static and obtuse.
- Prevent cookie replay attacks by verifying authentication cookie's last login time, which will only be given at login time, with the last login time stored in the database.
- To prevent sniffing that reveals MySQL commands and return queries between the web app and database servers, database servers and the web app will need to be configured to only accept remote connection via TLS1.3 and nothing lower.

3 Subsystem 3 (Researcher's Functionalities)

3.1 Overview

This subsystem will allow for researchers to retrieve and view anonymised records of patients who fit their search criteria and to retrieve an aggregated set of results. This subsystem has three parts to it - the generation of a large data-set, the implementation a k-anonymisation algorithm and the creation of several web-pages for researchers to access the anonymised records.

3.2 Claims and Assumptions

- Diagnoses and records will be treated as data and not quasi-identifiers.
- Records are assumed to have been de-identified.
- The time taken for the completion of the anonymisation algorithm on the data and the display of the records will lie within the researcher's expectation of waiting time.
- The researchers will only download records of a particular type at any one time.

3.3 Tools and Software

The tools and software used for this subsystem will be similar to the ones listed under 2.3.

3.4 Implementation

3.4.1 Data Generation

Generation of the basic information of user accounts can be done via a Python script with data pulled from the Internet.

In order to generate data with medical records that correspond to the diagnosis of a patient, we first select a set of diagnoses from ICD-10 2016. We then proceed to manually identify the records and the plausible readings for each diagnosis in the set.

After that, each patient will be randomly assigned to one of the diagnoses in the set. The relevant records will then be generated for that patient's diagnosis.

3.4.2 Anonymisation

Firstly, the data will be de-identified. Names, NRICs and addresses of patients will be removed.

Anonymisation techniques include *Generalisation* and *Suppression. Generalisation* involves replacing an individual value of an attribute with a broader range of values while *Suppression* refers to the omission of records whose set of quasi-identifiers appear in less than k records.

To achieve k-anonymity, the Datafly algorithm will be used. The Datafly algorithm is a greedy heuristic algorithm that achieves k-anonymity by generalising the quasi-identifier with the greatest number of distinct values. Following that, records which occur less than k times will be suppressed. Since the suppression of records is generally discouraged, a slight modification will be made to the algorithm to include a suppression threshold. Should the number of suppressed records exceed the threshold, further generalisation will be carried out on the data set.

Our decision to utilise the Datafly algorithm stems from the fact that it is relatively efficient and reliable as compared to other well-established k-anonymity algorithms.

Currently, the value of k is set to be 3 as that is the minimal recommended value and the suppression threshold to be at 5% of the total number of records.

3.4.3 Queries

The researcher will be able to retrieve records by entering either the age, nationality, sex, gender, postal code, record creation date or all of them. The diagnoses and the records will be loaded from the database. These data will then be run through the k-anonymisation algorithm. Relevant anonymised records will be retrieved and the researcher will be able to filter the records by their types such as blood pressure readings and X-rays.

On top of being able to retrieve individual records, researchers will also be able to request for summary statistics of readings. For example, they could request for the average blood pressure of residents of a particular postal code. In that case, they would enter the postal code into the search field. The average blood pressure reading of all records that are related to that particular postal code would be calculated. Should there exist only one record that fits the search query, that record will be suppressed and researchers will be informed that no relevant data is available.

3.4.4 Interface for Researchers

Researchers will have access to these pages:

- Dashboard

  Upon login, Researchers will first be presented with a dashboard showing the functionalities he is able to access and the pages of which these functionalities reside on.

- Aggregated Search

  On this page, researchers will be able to request for some of the summary statistics i.e. min, max and mean of the readings which are namely blood pressure, height, weight and BMI of patients that fit their search criteria.

  This page will consist of two drop-down menus and an input field. One would be a “Search By” menu which allows researchers specify the values of the different quasi-identifiers. The input field would enable the researcher to enter the search value. The other drop-down menu would be a “Reading Type” menu which enables researchers to specify the type of readings that they would like to have the summary statistics for.

  Upon clicking of the “Submit” button, the summary statistics of the requested readings of patients who reside in that location will be computed.

- Record Search

  On this page, researchers will be able to search for anonymised individual records that fit their search criteria. There will be two input fields, one for age and the other for the postal code, three drop-down menus, one for gender, one for sex, and the last one for the record type and another input field with a date picker to indicate the creation date of record.

  There will be another drop-down menu for researchers to specify the type of records that they would like.

  There will be a message on the page informing researchers that they will not be able to retrieve specific records as the results returned will be k-anonymised.

After clicking the 'Search' button, the quasi-identifiers, relevant records with the generalised quasi-identifiers will show up in the rows of the table.

If the record type is a reading, it will be displayed in the table. Else, a button 'View' will be available next to the record and a pop-up will show up displaying either a graph, an image, or a video.

Researchers would be able to click on the checkbox next to each of the records to select the ones that they want to download. A download button will appear next to the search button.

Clicking the 'Download' button will lead to the downloading of a csv file if the specified record type is a type of reading. Else, the 'Download' button will trigger the downloading of a zip file which consists the files of that record type.

3.5 Security Considerations

A cause of concern would be the possibility that attackers could input values for the different quasi-identifiers separately. There could be a correlation between the tables that are generated each time and this could lead attackers to infer certain sensitive information. To mitigate this problem, we intend to run the k-anonymity algorithm on all records in the database each time the "Search" button is clicked on.

4 Subsystem 5 (Data Collection from Sensors)

4.1 Overview

In this subsystem, user is able to securely upload medical data (i.e. sensor readings, images and videos) from his local device (Android phone) to the database. Regarding the design purpose of this subsystem, only two types user, patient and therapist, are allowed to upload medical data to the database from their phone. A patient can upload data for himself using patient's mobile device and NFC tag, while a therapist can upload data for his patients using therapist's mobile device and the patient's NFC tag, under the condition that the patient is unconscious and therefore unable to upload data by himself.

User is able to upload all types of medical data from his device, including readings, time series data, images, videos and documents. However, user can only upload files with certain extension types (i.e. .docx, .png, .mp4) restricted by the system via the record type stipulated, on top of system wide policies. Otherwise, if user intends to upload some sensor data (i.e. heart rate, blood pressure, daily steps) without any file attached, he can directly enter the data content in the application and upload. The checking of file extension will additionally be performed on the web app via header inspection.

4.2 Claims and Assumptions

- All the medical data to be uploaded, including files and sensor data, are already stored in user's local device.
- The therapist taking care of the unconscious patient is able to get the patient's NFC tag so that he can perform authenticated data uploading.

4.3 Tools and Software

- Android phones (at least version 4.0.3) with in-built NFC reader which have been registered in the system
- NFC tag of therapist or patient

4.4 Implementation

4.4.1 Data Collection / Retrieval

1. Medical data files are assumed to be originally taken and stored in the mobile device instead of retrieving from other remote sources. For example, image and video records are taken using phone's camera and video recorder, and therefore auto-stored in the local storage of the phone.
2. Sensor data can be collected using sensor applications in the phone or remote sensor devices (i.e. Fitbit). This kind of data may not necessarily be stored somewhere in the phone if it is just values instead of contained in a file. User can just get the values and enter it manually in the application when uploading data.

4.4.2 Data Upload by Patient

1. Patient clicks "Upload Record" button in the mobile app as described in 1.4.4.
2. Patient enters information about the record to be uploaded:

   (a) Record title

   (b) Medical type (select from the list)

   (c) (optional) Associated diagnosis

3. Patient chooses the mode of uploading the record:

   (a) If patient chooses to upload record by file, then he is required to select a file from the local storage of his device. The system will reject the file if the extension format is unsupported.

   (b) If patient chooses to upload record by content, then he is required to manually enter the data value to the content input field provided by the application.

4. Patient requests to upload the record and is prompted by the web server to scan his NFC tag using the mobile application for authentication.

5. Patient scans his NFC tag to generate digital signature for the record, and then sends the record with the signature to the web server (secured by TLS).

6. Web server checks the authenticity of the record, and checks for potential viruses contained in the record.

7. Once the record is verified valid, web server will properly store the record information in the database.

8. Web server notifies the patient that medical record has been uploaded successfully.

4.4.3 Data Upload by Therapist for Normal Patient

1. Therapist clicks "Upload Record (for Patient)" button in the mobile app as described in 1.4.4.

2. Therapist enters information about the record to be uploaded:

   (a) Patient that owns the record

   (b) Record title

   (c) Medical type (select from the list)

   (d) (optional) Associated diagnosis

   (e) (optional) Remarks

3. Therapist chooses the mode of uploading the record:

   (a) If therapist chooses to upload record by file, then he is required to select a file from the local storage of his device. The system will reject the file if the extension format is unsupported.

   (b) If therapist chooses to upload record by content, then he is required to manually enter the data value to the content input field provided by the application.

4. Therapist requests to upload the record and is prompted by the web server to scan the his NFC tag using his mobile application for authentication.

5. Therapist scans his NFC tag to generate digital signature for the record, and then sends the record with the signature to the web server (secured by TLS).

6. Web server checks:

   (a) The authenticity of the record (whether the record is created by the therapist)

   (b) The permission of the therapist (whether he is allowed to upload record for the patient)

    (c) Potential viruses contained in the record

7. Once the record is verified valid, web server will properly store the record information in the database, under the patient's account.
8. Web server notifies both the therapist and the patient that medical record for the patient has been uploaded successfully.

4.4.4 Data Upload by Therapist for Emergency Patient

1. Therapist clicks "Upload Record (for Emergency Patient)" button in the mobile app as described in 1.4.4.
2. Therapist enters information about the record to be uploaded:
    (a) Patient that owns the record
    (b) Record title
    (c) Medical type (select from the list)
    (d) (optional) Associated diagnosis
    (e) (optional) Remarks
3. Therapist chooses the mode of uploading the record:
    (a) If therapist chooses to upload record by file, then he is required to select a file from the local storage of his device. The system will reject the file if the extension format is unsupported.
    (b) If therapist chooses to upload record by content, then he is required to manually enter the data value to the content input field provided by the application.
4. Therapist requests to upload the record and is prompted by the web server to scan the patient's NFC tag using therapist's mobile application for authentication.
5. Therapist scans patient's NFC tag to generate digital signature for the record, and then sends the record with the signature to the web server (secured by TLS).
6. Web server checks:
    (a) The authenticity of the record (whether the record is owned by the patient)
    (b) Whether the record creator is the therapist associated with the emergency patient
    (c) Potential viruses contained in the record
7. Once the record is verified valid, web server will properly store the record information in the database, under the patient's account.
8. Web server notifies the therapist that medical record for the patient has been uploaded successfully.

4.5 Security Considerations

Since the system is using TLS1.3 for communication and data transfer, it ensures the authentication of the web server to the client, as well as the confidentiality and integrity of data transmitting between the web server and client. Therefore, attacker is unable to sniff the content of the record during transmission, or to capture the packets and perform replay attacks.

To ensure that the record being uploaded belongs to a particular patient, NFC tag is used to check the authenticity of the uploader or the record under different conditions. When patient tries to upload record for himself or therapist tries to upload record for his emergency patient, the patient's NFC tag is required to authenticate the record. When therapist tries to upload record for his normal (conscious) patient, the therapist's NFC tag is required to validate the permission of the therapist. After the therapist has been verified, the web app will be responsible for assigning the ownership of the record to the particular patient. The data related to the record will be then be expunged from the Android app.

-End-