PRIVACY-PRESERVING BASED ACCESS CONTROL FOR HEALTH INFORMATION NETWORK

ระบบควบคุมการเข้าถึงเวชระเบียนระหว่างโรงพยาบาลด้วยนโยบายความเป็นส่วนตัว

BY

MISS CHIDCHANOK	**BUNJONGPEAN**	**6088012**
MISS ARIZA	**DOLSOOKLERT**	**6088037**
MR. JIRAPUT	**THAMSONGKRAH**	**6088198**

ADVISOR
DR. ITTIPON RASSAMEEROJ

A Senior Project Submitted in Partial Fulfillment of the Requirements for

THE DEGREE OF BACHELOR OF SCIENCE (INFORMATION AND COMMUNICATION TECHNOLOGY)

Faculty of Information and Communication Technology
Mahidol University

2020

CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

CHAPTER 1
INTRODUCTION

As technology is currently evolving, the way to communicate is also increasing which makes it easier to violate personal information right. Medical information is considered to be one of the information that has been violating the patient's personal information right. Medical information is a record that keeps all the patient's information, patient's treatment history, patient's disease along with the patient's family information as well. It is considered to be important information for patient treatment and in the law area as well. In most of the hospitals, the patients do not have any authorization to access their medical information but all of the medical staff have access to their medical information even though the patient did not give any consent for them to be able to read the information. Moreover, the patient may not have treatment with only one hospital. It means that the patient's information will be scattered and it will be hard to update all the medical information. Also, it will be hard for the patient when they need to ask for the medical information from one hospital and bring it to another hospital which they have to do by themselves.

1.1 Motivation

A patient does not have access to their medical information, but the hospital staff is able to access which it may violate the personal information right. Moreover, if the patient needs their medical information to do treatment in another hospital, they will have to go to that hospital and ask for the information by themselves, which wastes a lot of time. This application will help solve the problems. The system will have an authentication system and authorization system for the patients to use which helps the patient have more convenience and be more secure by restricting the Personal Data Protection Act (PDPA).

1.2 Problem Statement

Managing the medical records of the patient according to the General Data Protection Regulation (GDPR) or Personal Data Protection Act (PDPA) is quite difficult because the patient cannot access their own record that has been kept by the hospital. They cannot give any authorization to the person who can access the information, but the medical staff can access all the data. Moreover, if the patient wants to ask for the medical record, they will have to ask the hospital directly and the patient will never know who can access their information and how secure their information is.

Furthermore, most hospitals have their own account management systems for the patient to register and keep their medical information. However, one patient can visit more than one hospital, which each hospital will have their own account management and authentication systems that will make it more difficult and inconvenience for the patient when they need to use and get into their medical information. Also, most hospitals do not have a good access control model, so the medical staff can see the patient's medical information only within the hospital, which makes it more difficult if the patient has their last medical record in another hospital.

1.3 Objectives of the Project

The purpose of this project is mostly for the patients of the hospitals.

- To help the patients have full access to their medical information through the Internet.
- To help the patients be able to have rights to give access to their medical information with the related medical staff from all hospitals that they visit.
- To ensure the privacy of the patient's medical information and lift up the security standard of storing, using medical information.

1.4 Scope of the Project

This project is a web-based application. Both patients and the medical staff will access the website itself. Scopes of this project are as follows:

- The application will have authentication and authorization system based on the PDPA law.

- The medical staff in a hospital can access a patient's information from other hospitals conveniently and securely under the authorization of the patients. (Right to Object).
- The hospital database must be kept in the format of SQL.
- Initially, this application will be used with Ban Praew Hospital, Nakhon Pathom Hospital, and Sam Pran Hospita.
- There will be a little or no changes to the current systems of the hospitals.

1.5 Expected Benefits

This project will benefit patients the most. The patients will be able to access their information and give authorization to any doctors through our application. The expected benefits of this project would be as follows:

- The system will provide accurate, up-to-date, and complete information about patients at the point of care.
- The system will allow patients to have quicker access to their record. Moreover, all of the patient's records will conceptually be in one place. (efficient care)
- The system will allow the patient to share information with other clinicians securely.
- The system will provide more effective diagnosis, reduce medical errors, and provide safer care to patients.
- The system will improve the interaction and communication between patients and doctors, as well as health care convenience.
- The system will enable a safer and more reliable method to share medical information.
- The system will enhance the privacy and security of patients' data.
- The system will help improve productivity and work-life balance.
- The system will reduce the costs by decreasing the paperwork, improve safety, and reduce duplication of testing.

- This system will help raise the standard of storing and accessing medical information.
- This system will help raise the security awareness of both patients and medical staff members.

1.6 Organization of the Document

This document consists of six chapters including:

1. Introduction – It contains the introduction of this project including motivation, problem statement, objectives, scope, expected benefits, and organization of the document
2. Background – It introduces a fundamental of the related documents which contain several background requirements of project development.
3. Analysis and Design – It describes the rationale and methodology of the project. There is a brief explanation in the architecture overview which illustrates a system flow of this project. Moreover, it provides several diagrams with a concise explanation to describe a workflow.

CHAPTER 2
BACKGROUND

This chapter consists of five main chapters including Personal Data Protection Act (PDPA), terminology, techniques and technologies, tools, literature review in order to provide essential information to support this project.

2.1 Literature Review

2.1.1 A framework for privacy-preserving healthcare data sharing

This paper has focused on creating a framework for privacy-preserving data sharing. [1] It has a total three main focuses which are meaning of privacy, privacy preservation policy, and privacy conservation sharing health information. The framework provides a solution to solve the conflict. It has a based identifier to identify and map with the health care data. Common privacy policy that will be used to identify the user whether they have the access or not. It also has a different kind of way of sharing the data. If the portion of the data is large, the K-anonymity model will help handle the data properly which helps make the data become anonymous. The framework could help in tracing and characterising the data also limiting the access and able to check who access the data.

2.1.2 A Framework of Access Control Model on Cross-Entropy in Health Information System

The authors have created the framework based on the access control model which uses the doctor's access record to determine the risk in accessing the data [2]. The risk evaluation has been calculated by evaluating the internal and external conditions. It also has been calculated based on three main values which are "Risk Quantification", "Risk Aggregation", and "Risk Level". Cross-entropy has been used in this paper to calculate the risk criterion and specify the risk. If the risk evaluation is too high, the access will be denied and the risk guideline will be endorsed.

2.1.3 A Secure and Flexible e-Health Access Control System wil Provisions for Emergency Access Overrides and Delegation of Access Privileges

In this paper, the authors have tried to find the way for the e-Health access control system to be more secure and more flexible to help the system access become more robust and there is a determination aware of the emergency circumstances [3]. The author has used many methods to improve the system in this paper. For example, the author uses the RBAC model to map the roles and permissions of the user or uses the context-policy to deal with the repository. For authentication, the author uses the eTRON security architecture which comes with a card that could be used to identify the owner and the issuer of the card. For the authorization, the author had established a secure system that could verify the person who is accessing the e-Health system.

2.1.4 ACTION-EHR: Patient-Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care

The authors have established a system that is secure and can easily manageable and trustable for the electronic health record or EHR. Moreover, the established system grants the patient to be able to manage their own health record across numerous hospitals [4]. The system uses the blockchain as their main implementation. Blockchain has been used to store the metadata and other data will be stored on a cloud-based repository. For security, the author chose to use the public key infrastructure asymmetric encryption and digital signatures to protect the EHR data.

2.1.5 An OpenNCP-based Solution for Secure eHealth Data Exchange

The authors have developed the outcome of OpenNCP from a sound holistic access to secure at a systemic level [5]. The author also uses the KONFIDO approach to making sure that the health-care data transaction to Europe is being protected. Blockchain has been used in this paper as well. It is used to see whether the request was sent by the authorized user or not.

2.1.6 Blockchain-Based Personal Health Records Sharing Scheme with Data Integrity Verifiable

The authors have found a way to share personal health records in order to improve doctor diagnosis [6]. However, patients cannot be able to control their personal health effectively. In addition, the cloud service provider can alternate the health record. The author uses blockchain for integrity purposes. Blockchain provides integrity verifiable and decentralized management. Moreover, it can prevent a single point of failure with blockchain. The author stores the hash value of personal health records in the blockchain. In a smart contract, the author stores the index set. This can improve data integrity effectively.

2.2 Personal Data Protection Act (PDPA)

Personal Data Protection Act or PDPA is an act that aims to secure the personal data of users [7]. At the end of May 2020, it was announced officially. The PDPA will help develop data privacy rules, including the preservation of data, the use of data. The primary purpose of PDPA is to protect the data that could identify the data owner. Name, address, e-mail address, telephone number, identification number, including your fingerprint, for example. A significant part of the act is a set of rights that apply to businesses as well as individuals. The rights include [8]:

2.2.1 Right to access

The owner of the data will have the right to access the data and be able to get the copy of that data. As well as having the right to ask how their data was retrieved in the case that they are unsure whether they give the right to access their data. The right to that data must not contrary the law and that right must not violate the rights of other people.

2.2.2 Right to data portability

In the case that the owner of the data wants to transfer the data from one data keeper to another, the data's owner can ask the data keeper to send or transfer the data directly. The right must not contrary the law, contract, or violate the rights of other people.

2.2.3 Right to ensure/ Right to be forgotten

If the data keeper shares the data in public or easy to access the data, the owner of the data has the right to ask the data keeper to delete, destroy that

data, or make the data unidentifiable. The data keeper will be the person who takes full responsibility taking care of the request including all the costs that occur.

2.2.4 Right to be informed

The data keeper must inform the data owner all the details on collecting the data and how the data is going to be used. The data owner has the right to know the objective of collecting the data, how the data is going to be used or sharing the data, what needs to be collected, the period of collecting the data including the contact of the data keeper. Moreover. The data owner must know the consequence of not giving the data to the data keeper.

2.2.5 Right to object

The data owner has the right to oppose collecting the data, use, or sharing the personal data whenever they want including making the data become unidentified.

2.2.6 Right to rectify

The data owner has the right to ask to edit the data to make it right, make it uptodate and not make it confusing which act of editing the data must go according to goodwill and not violating the law.

2.2.7 Right to restrict processing

The data owner has the right to ask the data keeper to restrain from using the data for any reason even for the change of mind or decide not to destroy the data when the deadline of destroying the data due to the data owner must use the data with the law.

2.3 Terminology

2.3.1 Authentication

Authentication is “the process of recognizing a user’s identity” [9]. It is the mechanism whereby an incoming request is paired with a collection of credentials. The credentials supplied are compared to those on a file on an authenticated user’s database with information on a local operating system or on an authentication server. A user provides an identifier to signify the account they wish to use and enters login credentials for the account. The

credential may involve something that the user knows such as password, something the user has such as numeric code.

2.3.2 Authorization

Authorization is an “official permission for something to happen, or the act of giving someone official permission to do something” [10]. When an account is created, it is often necessary to specify what the account can do, in the form of privileges. Authorization has been used for granting privileges that govern what an account is allowed to do.

2.3.3 Medical Information

Medical Information is the collection, handling and dissemination of information on medications, and their safe and correct use [11].

2.3.4 Medical Record

The document explains all details about the patient's history, clinical findings, diagnostic test results, pre and postoperative care, patient's progress and medication [12]. However, in this project, ‘Medical Record’ will only refer to patient basic information.

2.3.5 Medical Staff

In this project, ‘Medical Staff’ includes physicians, dentists, nurses, and other professional individuals who have admitting privileges to the hospital [13].

2.4 Techniques and Technologies

2.4.1 Authentication System

Authentication system is the system that acts as the barrier of the software. It makes sure that the system and the information can only be accessed by the right person [14]. It is considered to be a very important system for organization because it helps the organization to make sure that their information and resources are secure and only the related people can access to their information and resources [15]. Authentication system could be more than just a simple HTML login page. It could be OpenID connect or cookie/session based to communicate between different authentication systems in different organizations.

2.4.2 Sensitive Data Management

Sensitive data is "an information that must be protected against unauthorized access [16]." Access to sensitive information ought to be restricted through sufficient data security and information security. Practices designed to forestall unauthorized revealing and data breaches. Sensitive information can embody info that may hurt an individual or their reputation, together with information concerning health, criminal record, or behaviors. Managing the sensitive data is considered to be important. It could make use of passphrase, encryption, access control, and user authentication to supply a secure answer to managing sensitive information. It is extended to guard the integrity of the configuration files, to secure the configuration process, and to support secure sensitive information or SSD zero-touch auto configuration [17].

2.5 Tools

2.5.1 HOSxP on Windows 7

HOSxP is a system that works on Microsoft Windows operating systems. It is a windows application software that is created for hospitals, health stations, or clinics. The system could link all of the information within the hospital efficiently for the convenience of the patient and to dissolve the complexity of each department [18]. However, we only use the HOSxP as a system and database scheme references for this project.

2.5.2 MariaDB on Windows7

MariaDB is "an open-source, multi-threaded, relational database management system [19]." It is one amongst the foremost common open-source SQL relational databases management systems. It is designed for reliability, easy use, and therefore the most prominent feature is its speed [20]. Also, it may manage small amounts of information quickly and smoothly, creating it convenient for little businesses or personal projects. It uses a client/server model with a server program that files requests from client programs and the server and the client programs can be on different hosts. MariaDB is very compatible with MySQL. It supports various SQL statements, structure, and rules, functions and procedures, user-defined

functions, server variables, and SQL modes. From the existing system, they use MariaDB for storing the personal health record in the hospital in order to manage the patient information.

2.5.3 Protocols

2.5.3.1 Single Sign-On (SSO)

Single sign-on is “an authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials [21].” It is the ability to log in once and so access further protected resources or applications with similar authentication requirements, while not having to re-enter credentials [22]. It works depending on trust relationships built up between applications. It is often based on certificates that alternate between the identity supplier and therefore the service provider. The certificate will be accustomed to sign identity data that is being sent from the identity provider to the service provider so the service supplier is aware that it is coming back from a reliable source. The identity data takes a scheme of tokens that contain distinguishing bits of data concerning the user sort of a user’s email address or a username.

2.5.3.2 OpenID Connect (OIDC)

OpenID Connect or OIDC was designed to supply a key feature required for authentication service. It permits users to verify the identity of the end-user supporting the authentication performed by an authorization server, additionally to acquire basic profile information concerning the end-user during a practical way [23]. OIDC can facilitate the system to receive the data easier while not having too many steps [24]. It was designed as a layer on top of the OAuth 2.0 protocol to provide information in a definitive format to applications about the identity of an verify user, OIDC allows users of all types, together with web-based, mobile, and JavaScript users, to request and receive information concerning verify sessions and end-users. It permits the participants to use alternative options like coding of identity information discovery of

OpenIS providers, and session management, once it is sensible for them [22].

2.5.3.3 OAUTH 2.0

OAuth 2.0 is a protocol that permits a user to grant a third-party website or application access to the user's protected resources, while not essentially revealing their abiding credentials or maybe their identity [25]. It allows a user to authorize one application to send inquiry to the associated degree API on the user's behalf to retrieve information at the resource server in hand by the user. It builds a trust on HTTP that links to the application and also the personal information [24]. The request can incorporate the access token that is received from the application and interaction with the user. The application interacts with an authorization server that authenticates a user as a part of attaining their consent for the application to access their resources. The application receives a token which allows it to hail the resource server on the user's behalf [22].

2.5.3.4 SAML 2.0

Security Assertion Markup Language or SAML 2.0 is a standardized way to tell external applications and services that a user is who they say they are. It makes Single Sign-On or SSO, technology by providing a way to authenticate a user once and so communicate that authentication to multiple applications. It creates plenty of trust on the digital signature and SAML 2.0 token that is created by the supplier within the format of XML [24]. Application can verify the signature with the certificate. The data of the user are enclosed in the SAML token.

2.5.4 Public Key Infrastructure (PKI)

Public Key Infrastructure or PKI is a technology for authenticating users and devices within the digital world [26]. Its concept is to own one or additional trusted parties digitally sign documents certifying that a specific cryptographic key belongs to a particular user or device. The key will then be used as an identity for the utilization in digital networks. It helps create information and communication technology more protected and additionally

permits the use of public key cryptography in open computer networks, specifically on the internet [22].

2.5.5 Web Application Programming Tools

2.5.5.1 Node.js

Node.js is an open source, cross-platform runtime environment for developing server-side and networking applications. It is written in JavaScript language and can be run in Node.js runtime as well. It conjointly provides lots of libraries of varied JavaScript modules that simplifies the increase of web applications exploitation Node.js to a good extent [27].

2.5.5.2 React.js

React.js is “a declarative, efficient, and flexible JavaScript library for building user interfaces [28].” It will compose a complicated UI. It is an open source, front end, JavaScript language for building user interfaces. It is used as a base within the development of single-page or mobile applications [29].

2.5.5.3 Firebase Authentication

Firebase Authentication provides backend as a service, easy-to-use SDKs, ready-made UI libraries to authenticate users with the application [30]. It supports authentication in many forms such as passwords, phone numbers, or even federated identity providers like Google or Facebook. It combines with other Firebase services, and it has an advantage on industry standards like OAuth 2.0 and OpenID connect which it could easily incorporate with the custom backend. It creates SDK for Android, iOS, and web applications to use which it could handle signing in from many platforms such as social networks, email addresses, or even from anonymous people [31].

2.5.5.4 **PostgreSQL**

PostgreSQL is a tool that is used to manage the data in an object-relational database which it could use with almost every SQL language. It is an open source tool that could work on many operating systems such as Linus, UNIX, and Windows [32]. Moreover, PostgresSQL works best on OLTP/OLAP operation when it is being used to read, write, or analyse data. It also has its own security system called SE-PostreSQL and it uses SSL to connect with the client and server [33].

CHAPTER 3
ANALYSIS AND DESIGN

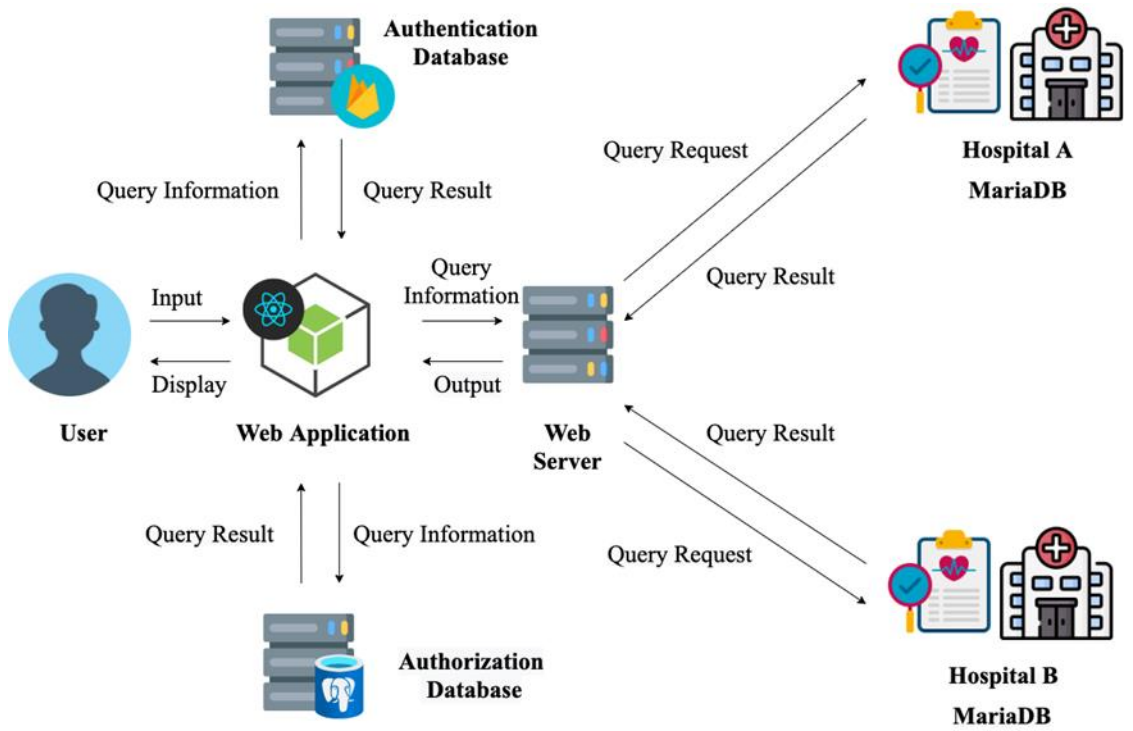
This chapter describes the analysis and design used to develop the application. Our Privacy-preserving Based Access Control for Health Information Network called Privame consists of system architecture overview, system structure chart, process analysis, database analysis, and user interface and flow diagram.

3.1 System Architecture Overview

The system architecture which is illustrated in Figure 3.1 consists of two main parts which are a web application and hospital databases from the existing system. The web application contains a database and web server for querying the data from the hospitals to manage the permission of the medical records. The user will be using the web application to input the information, give authorization, and the information will be displayed through the web application. All of the hospitals will access through the server which acts as the medium. If the user wants to get the information from the hospital, the server will send the query request to that hospital and the server will send the result back.

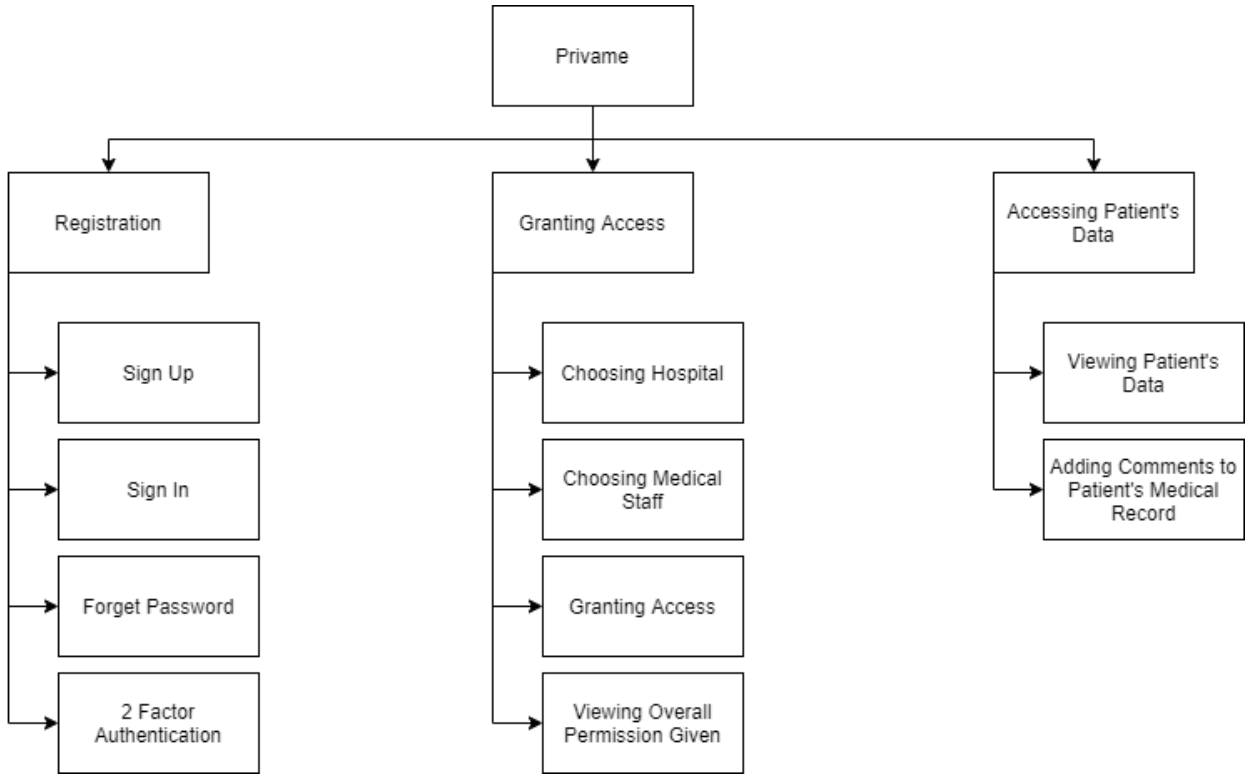
3.2 System Structure Chart

Our application will consist of three main functions as illustrated in Figure 3.2. Starting from our first function, Registration, the patient will be able to sign up, sign in, forget the password, including 2 Factor Authentication. The Next function is Granting Access, the patient can decide which hospital and which medical staff that the patient wants to grant access to. Furthermore, the patient can decide what level of access the medical staff can have, and the patient can also view all access granted. For our final function, Accessing Patient's Data, the medical staff can view the patient's data based on the access granted from the patient. Moreover, the medical staff can add comments to the patient's medical record.



Project : Privacy-Preserving Based Access Control for Health Information Network **System :** Privame	**Major Advisor:** Dr. Ittipon Rassameeroj
Description : Overview of out system architecture and existing architecture.	

Figure 3.1: System Architecture Overview



Project: Privacy-Preserving Based Access Control for Health Information Network **System:** Privame	**Major Advisor:** Dr. Ittipon Rassameeroj
Description : System Structure Chart of our system.	

Figure 3.2: System Structure Chart

The detailed description of each subsystem is shown below:

1. Registration – The registration function allows the user to either sign up or sign in.

    1.1. Sign Up – The registration page for users to sign up to use the system.

    1.2. Sign In – The registration page for the user who already sign up with Privame.

    1.3. Forget Password – When the user forgets their password, the user can user forgot password to reset the password.

    1.4. Two Factor Authentication – A function requires both the password and OTP to increase the level of security.

2. Granting Access – The function for the patient that allows the user to determine who can access their personal information.

    2.1. Choosing Hospital – Allows users to choose a collaborated hospital in order to specify whom to grant permission to.

    2.2. Choosing Medical Staff – Allows users to select which medical staff they would like to give the access to.

    2.3. Choosing Access – Allows users to choose the level of action that the medical staff can do with the patient’s medical record.

    2.4. Viewing Overall Permission Given – Allows users to review all the permission granted.

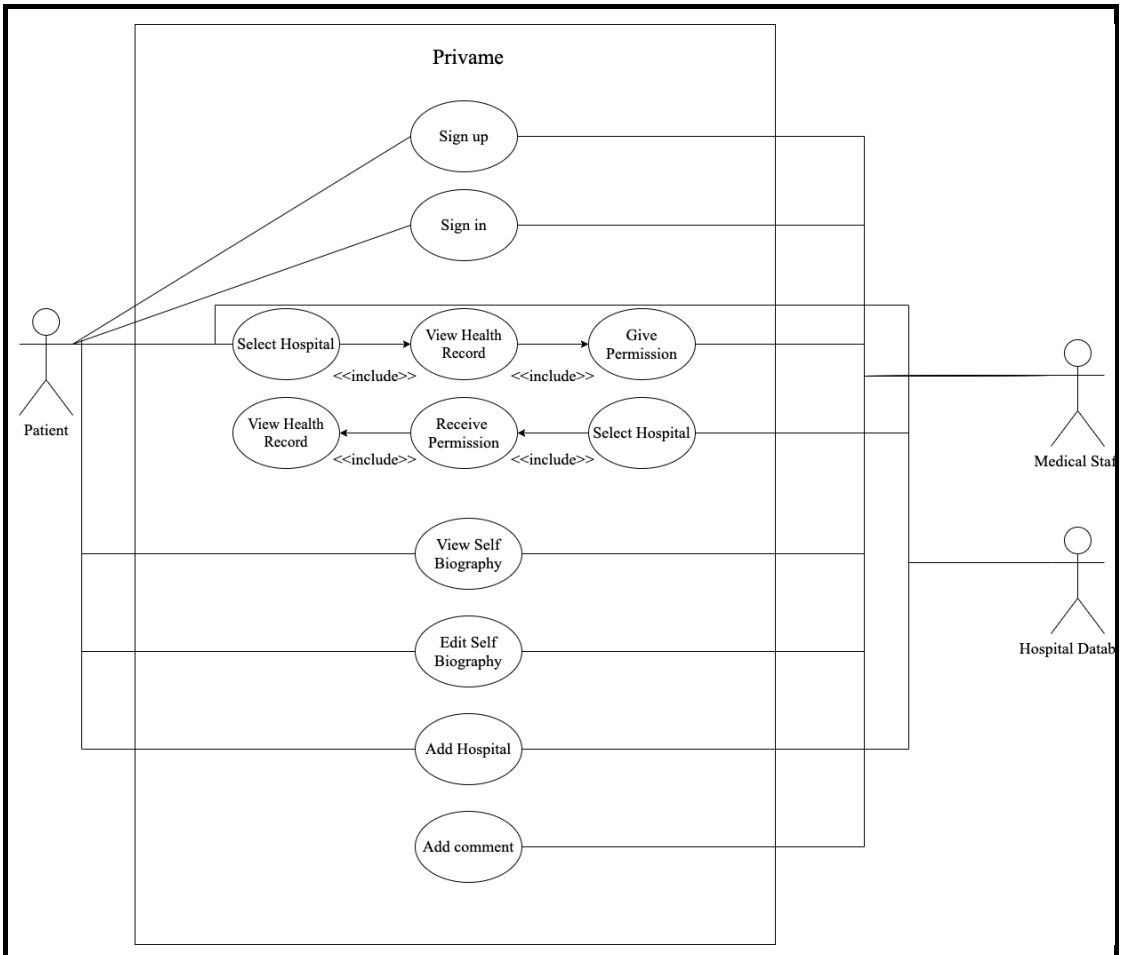
3. Accessing Patient’s Data – The function for the medical staff to access the patient’s medical information.

    3.1. Viewing Patient’s Data – The medical staff can view the patient’s data.

    3.2. Adding Comments to a Patient's Medical Record – The medical can add comments to the patient’s medical record.

Process Analysis and Design

3.2.1 Use Case Diagram



Project: Privacy-Preserving Based Access Control for Health Information Network **System:** Privame	**Major Advisor :** Dr. Ittipon Rassameeroj
Description : Use case diagram of our application.	

Figure 3.3: Use Case Diagram

In the use cases diagram, the actor consists of the patient and medical staff. All actors can sign-up, sign-in to the system, and view or edit their biography. After patients sign-in, they need to select and authenticate to the hospital by health number and birthdate in order to retrieve their personal health record from the hospital database and give permission to medical staff in the system. For medical staff, they need to select and authenticate to the hospital by medical number and birthdate in order to receive

permission from the patients. In addition, medical staff can add a comment on a shared personal health record from a patient, and the patient can view all given permission.

Table 3-1 to Table show the description of the system use cases

Table 3-1: Use Case Description (Registration)

Name	Registration
ID	1
Description	Patients want to use this system
Primary Actor	Patient, Medical Staff
Frequency of Use	Once, only the first time, when the user wants to register.
Triggers	Users would like to use Privame
Preconditions	Patients and medical staff must have at least 1 account with the hospital but never register with Privame.
Postconditions	Patients and medical staff got an account with Privame
Main Success Scenario	Patients and medical staff have data and health numbers in the hospital.
Alternative Flows	-
Exceptions	-

Table 3-2: Use Case Description (Authenticate to hospital)

Name	Authenticate to hospital
ID	2
Description	Patients and medical staff want to access their personal health record
Primary Actor	Patient, Medical Staff

Frequency of Use	Almost every time users would like to access Privame.
Triggers	-
Preconditions	Patients and medical staff must have already registered with Privame.
Postconditions	Patients and medical staff logged in to Privame.
Main Success Scenario	Patients and medical staff have retrieved the information from hospitals.
Alternative Flows	-
Exceptions	-

Table 3-3: Use Case Description (Give Permission)

Name	Give Permission
ID	3
Description	Patients want to share the personal health record to medical staff.
Primary Actor	Patient
Frequency of Use	Whenever patients would like to give access to the medical staff.
Triggers	When the medical staff need to access the patient's data.
Preconditions	Patients can access their personal health record.
Postconditions	The medical staff received the permission to access the patient's data.
Main Success Scenario	Patients shared the personal health record with the medical staff.
Alternative Flows	-
Exceptions	-

Table 3-4: Use Case Description (View Patient's Health Record)

Name	View Patient's Health Record
ID	4
Description	The Medical staff would like to view the patient's health record.
Primary Actor	Medical staff
Frequency of Use	Whenever the medical staff need to view the patient's health record.
Triggers	Whenever the medical staff need to view the patient's health record.
Preconditions	The medical staff must get the permission from the patient.
Postconditions	The medical staff viewed the patient's data.
Main Success Scenario	The medical staff is able to view the patient's health record.
Alternative Flows	-
Exceptions	-

Table 3-5; Use Case Description (View Self Biography)

Name	View Self Biography
ID	5
Description	Patients and medical staff would like to view their data.
Primary Actor	Patient, Medical staff
Frequency of Use	When patients and medical staff would like to view or check their data.
Triggers	-

Preconditions	Patients and medical staff must have already registered with Privame.
Postconditions	The biography has been viewed
Main Success Scenario	Patients and medical staff viewed their data.
Alternative Flows	-
Exceptions	-

Table 3-6: Use Case Description (Edit Self Biography)

Name	Edit Self Biography
ID	6
Description	Patients and medical staff want to edit their biography.
Primary Actor	Patient, Medical staff
Frequency of Use	Whenever there is an update on the biography or the data is wrong.
Triggers	The biography is needed an update.
Preconditions	Patients and medical staff must have already registered with Privame.
Postconditions	The biography has been updated.
Main Success Scenario	Patients and medical staff edited their biography.
Alternative Flows	-
Exceptions	-

Table 3-7: Use Case Description (Add Hospital)

Name	Add Hospital
ID	7

Description	A patient would like to sync their personal data with another hospital.
Primary Actor	Patient
Frequency of Use	Whenever a patient visits new hospital with collaboration.
Triggers	Patients visit new hospital
Preconditions	Patients must have the account in another collaborated hospital.
Postconditions	The new hospital has been added, and data has been joined.
Main Success Scenario	The patient's data has been synchronized.
Alternative Flows	-
Exceptions	-

Table 3-8: Use Case Description (Add Comment)

Name	Add Comment
ID	8
Description	The medical staff would like to add comment to the patient health record.
Primary Actor	Medical staff
Frequency of Use	Whenever the medical staff want to leave a comment after the diagnosis or treatment.
Triggers	After the diagnosis or treatment.
Preconditions	The medical staff must have the permission from the patient.
Postconditions	The comment has been added to the patient's medical record.

Main Success Scenario	The comment was added to the patient's medical record.
Alternative Flows	-
Exceptions	-

Table 3-9: Use Case Description (View all permission granted)

Name	View all permission granted
ID	9
Description	A patient would like to view all permission granted.
Primary Actor	Patient
Frequency of Use	Occasionally, Whenever the patient wants to review all permission granted.
Triggers	-
Preconditions	The patient must have an account with Privame.
Postconditions	-
Main Success Scenario	The permission granted has been viewed.
Alternative Flows	-
Exceptions	-

3.2.2 Data Flow Diagram

The data flow diagram illustrates the main processes of our web application as shown in Figure 3.4. The web application allows users to authenticate and give authority to other related authenticated users. For instance, authenticated users (patients) can assign permissions to their medical records for sharing data with the highest privacy.

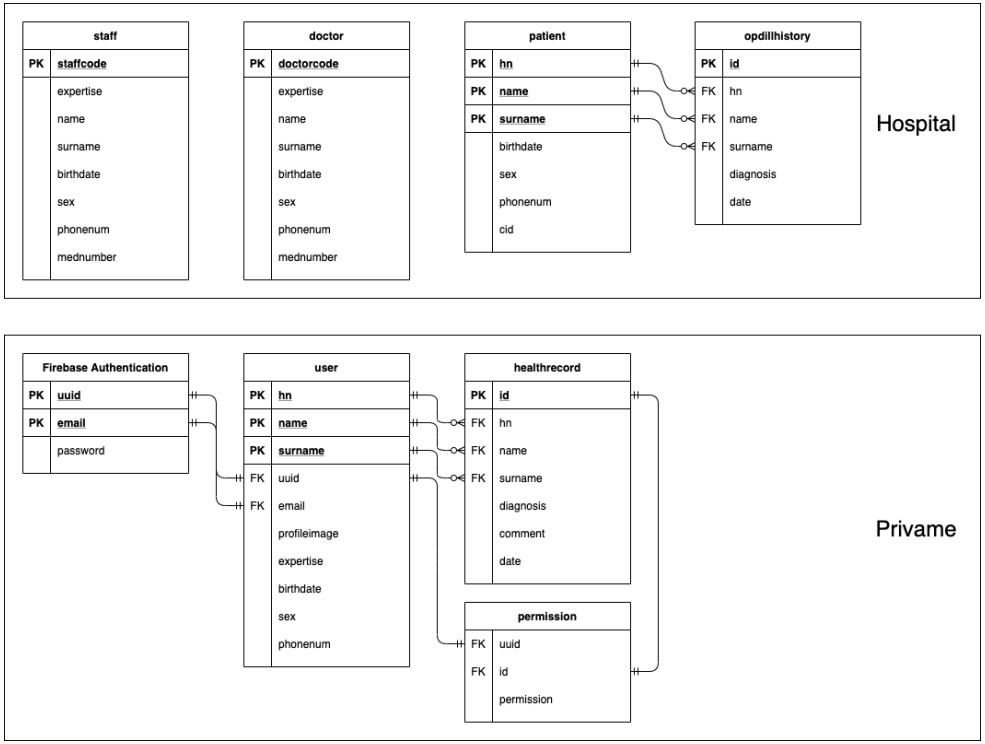
Project : Privacy-Preserving Based Access Control for Health Information Network **System :** Privame	**Major Advisor :** Dr. Ittipon Rassameeroj
Description : Data flow diagram of our application	

Figure 3.4 : Data Flow Diagram

3.3 Database Analysis and Design

3.3.1 ER-Diagram

The existing systems based on HOSxP consist of four tables which are staff, doctor, patient, and opdillhistory as shown in Figure 3.5. The staff table is information about staff in hospitals. The doctor table is information about doctors in hospitals. The patient table is the information of patients in hospitals. Opdillhistory table contains the information of patients in hospitals also known as a medical record. The web application consists of three tables which are user, healthrecord and, permission. Firebase Authentication is Backend as a Service from Google for accounting management. User table is used for collecting patient's and doctor's account information. The healthrecord table is used to store the patient’s health record from the hospital to this web application. The permission table is used for collecting permissions of medical records that patients will give access control to doctors. For example, which doctors can access which patients’ records



Project : Privacy-Preserving Based Access Control for Health Information Network **System :** Privame	**Major Advisor :** Dr. Ittipon Rassameeroj
Description : "<Short Description of the Figure Placed Above>"	

Figure 3.5: ER-Diagram

3.4 I/O Design

This section explains the design of the Input and Output User Interface. The section consists of two parts, the interface design and the transition diagram showing transition through the system.

3.4.1 Interface Design

Figure 3.6 shows the overview and flow of the application in two perspectives which are the medical staff's perspective and patient's perspective.

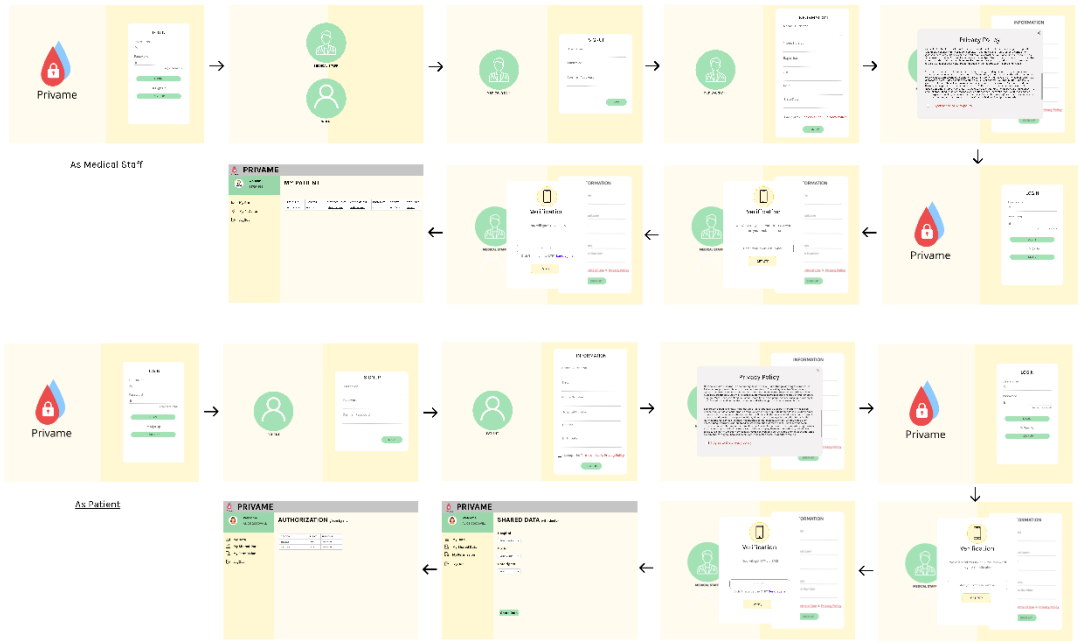


Figure 3.6: Interface Design Flow

This is the login page of the application. The user could login into the system directly if they already have the account. If the user does not have the account yet, they could click sign up to sign up for an account as shown in Figure 3.7.

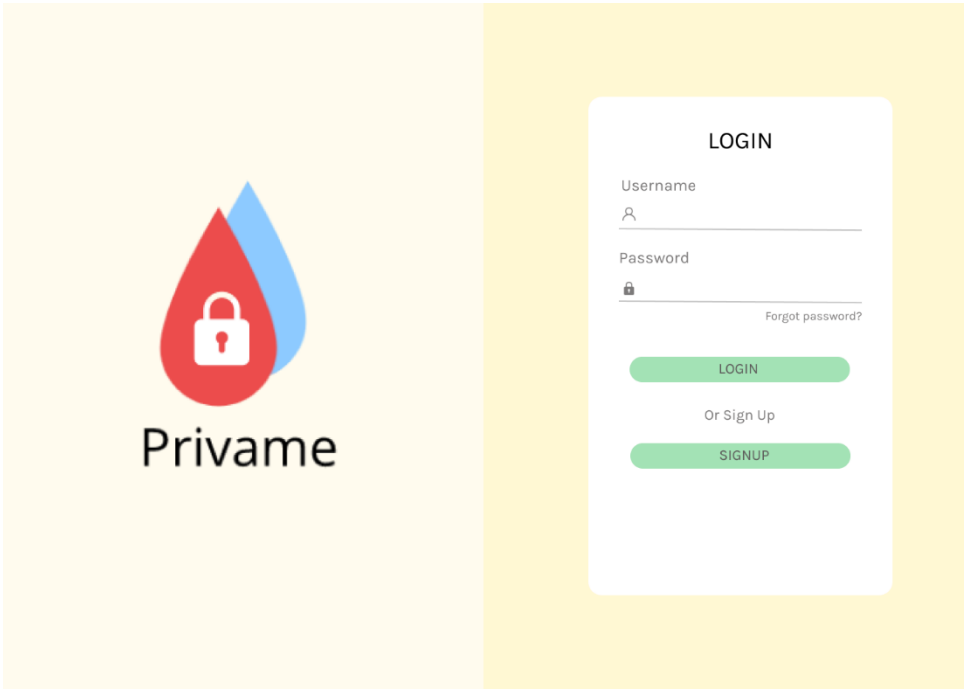


Figure 3.7: Login Page

This is a page after the user clicks the sign-up button. In this page, the user can select whether they are medical staff or patient which each one will link to a different sign up page as shown in the figure 3.8.

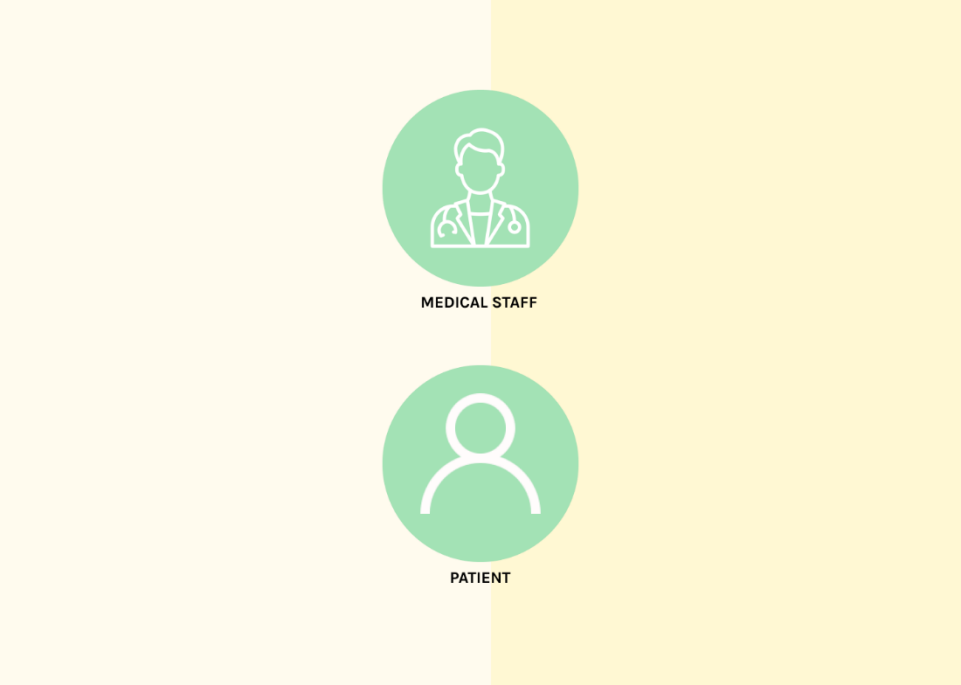


Figure 3.8: Choosing role to sign up

This page will show after the user chooses the role as medical staff. In this page, the user will have to input the username and password that they would like to use. Also, they will have to confirm their password as well as in Figure 3.9.

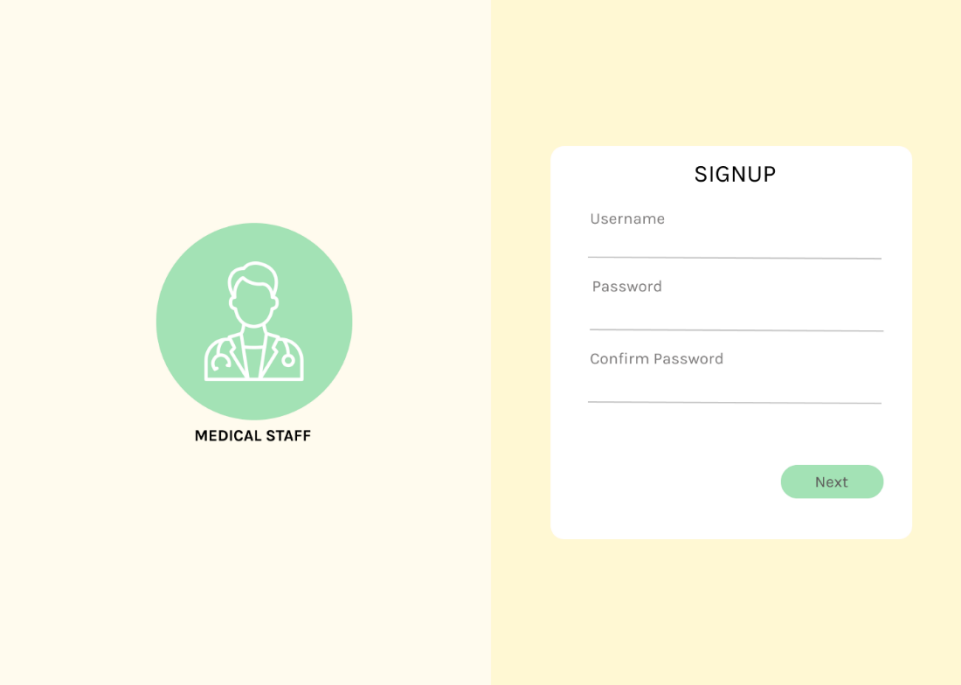


Figure 3.9: Medical staff role sign-up page

This page will come after the user chooses the role as medical staff and input the username and password. In this page, the user has to fill in all the basic information including name and surname, phone number, expertise, email address, role, and birth date. After the user has input all the information, the user must accept the terms of use and the privacy policy first before the user can click the sign up button as shown in Figure 3.10. The user can also click to see the privacy policy before clicking the accept button as shown in Figure 3.11.

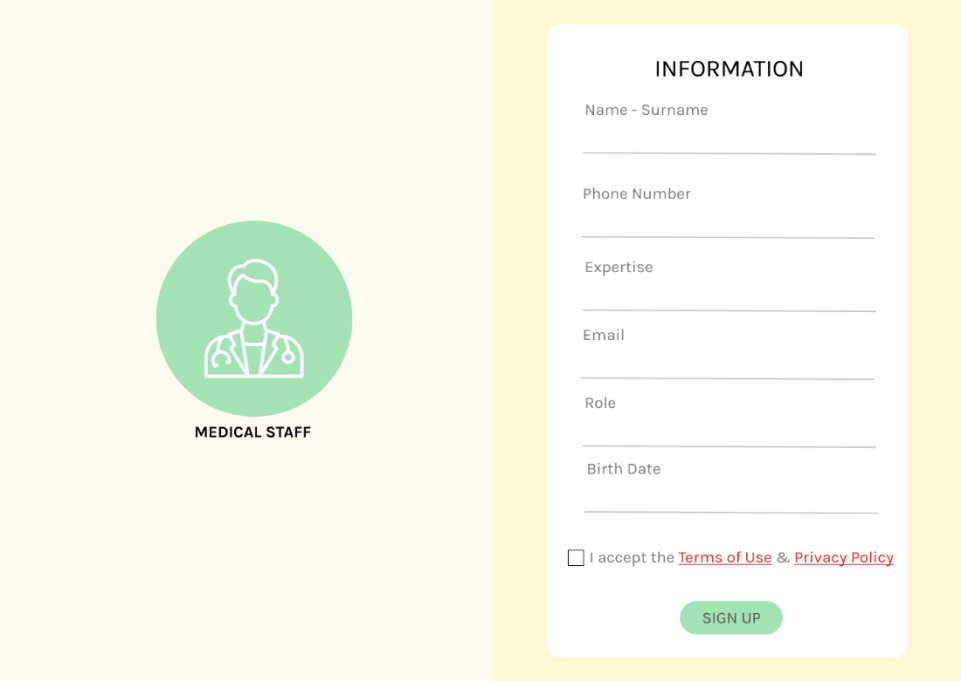


Figure 3.10: Medical staff role sign-up information page

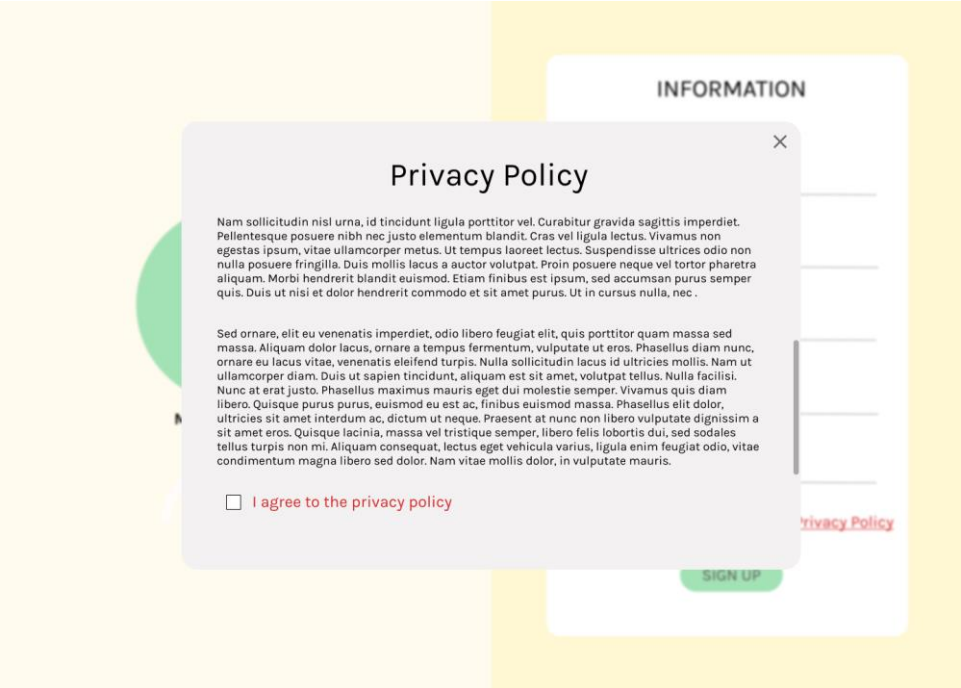


Figure 3.11: Privacy policy page

This page will show after clicking the sign-up button. It is the page for security which will make sure that it is really the user. The user has to fill in their phone number to be able to get the OTP code then click get OTP as shown in Figure 3.12. The number that the user chooses to receive OTP code must be the same phone number as the phone number that the user uses to register the account with the hospital. This will make sure that the user that is registering in the application is the same user from the hospital.

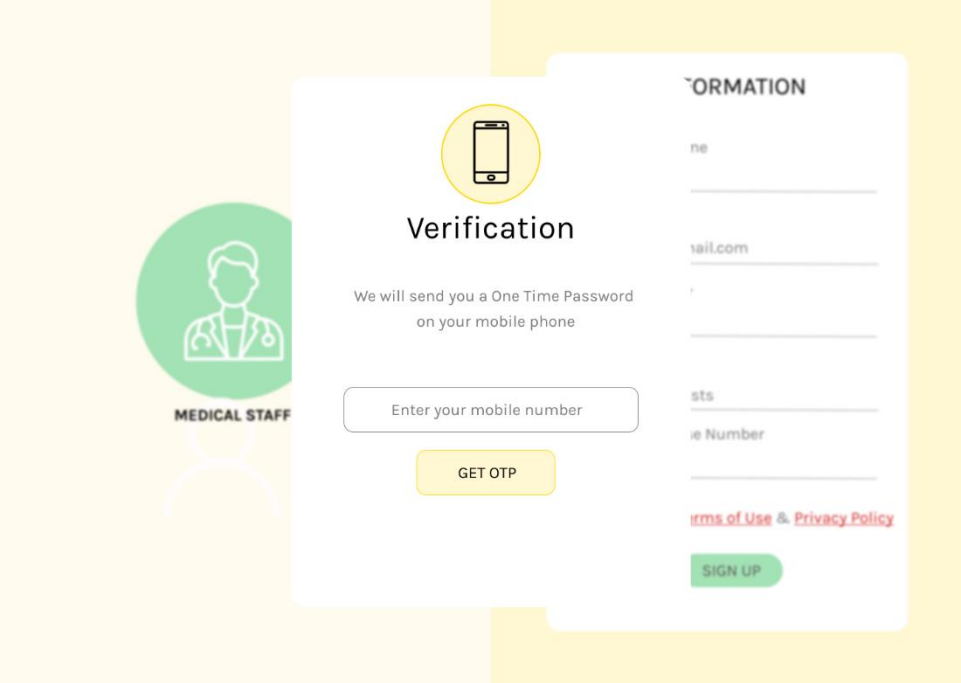


Figure 3.12: Verification request Page

This page will come after the user fills in their mobile phone number. The user will receive the OTP code via SMS then the user will fill in the code in the box then they could click the verify button as shown in figure 3.13.

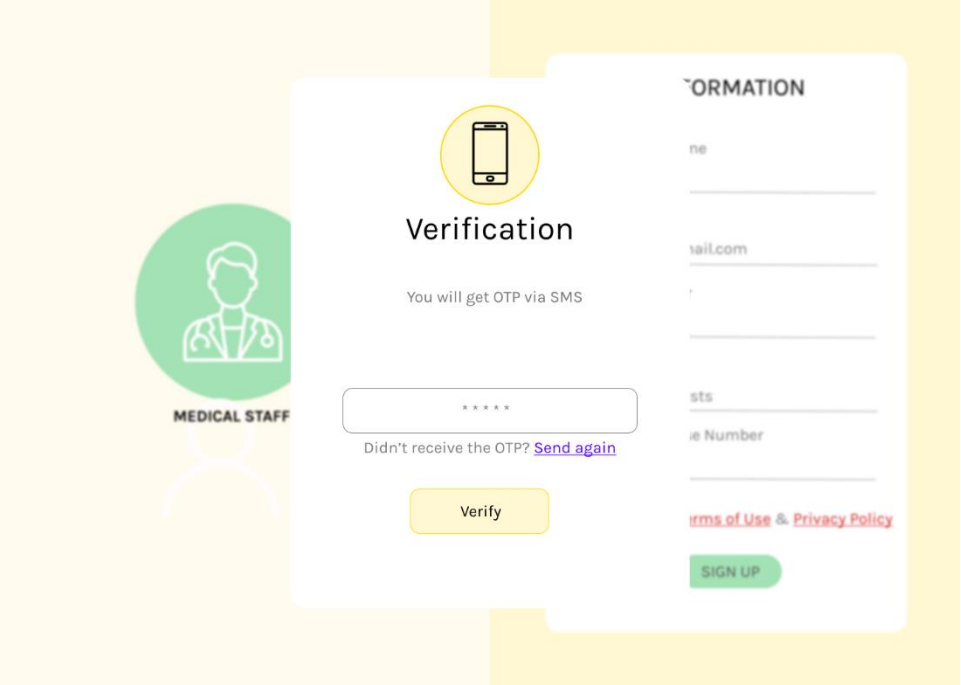


Figure 3.13: Verification Page

This page will show after the user chooses the role as patient. In this page, the user will have to fill in the username and password that they would like to use. Also, they will have to confirm their password as well as in Figure 3.14.

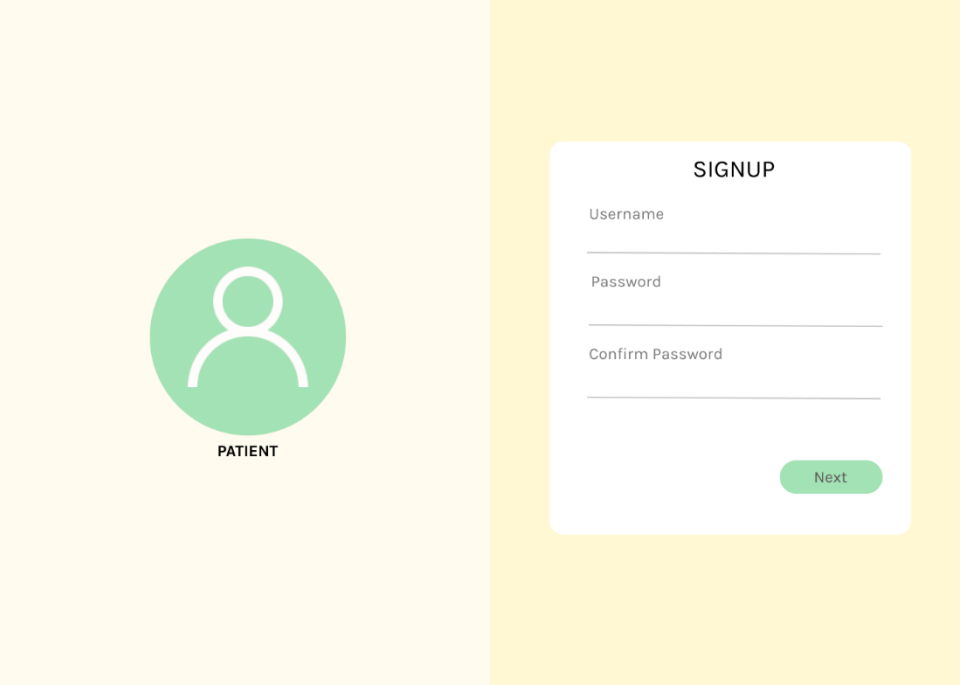


Figure 3.14: Patient role sign-up page

This page will come after the user chooses the role as patient and input the username and password. In this page, the user has to fill in all the basic information including name and surname, email address, phone number, hospital number, Gender, and Birth date. After the user has input all the information, the user must accept the terms of use and the privacy policy first before the user can click the sign-up button as shown in Figure 3.15. The user can also click to see the privacy policy before clicking the accept button as shown in Figure 3.11.

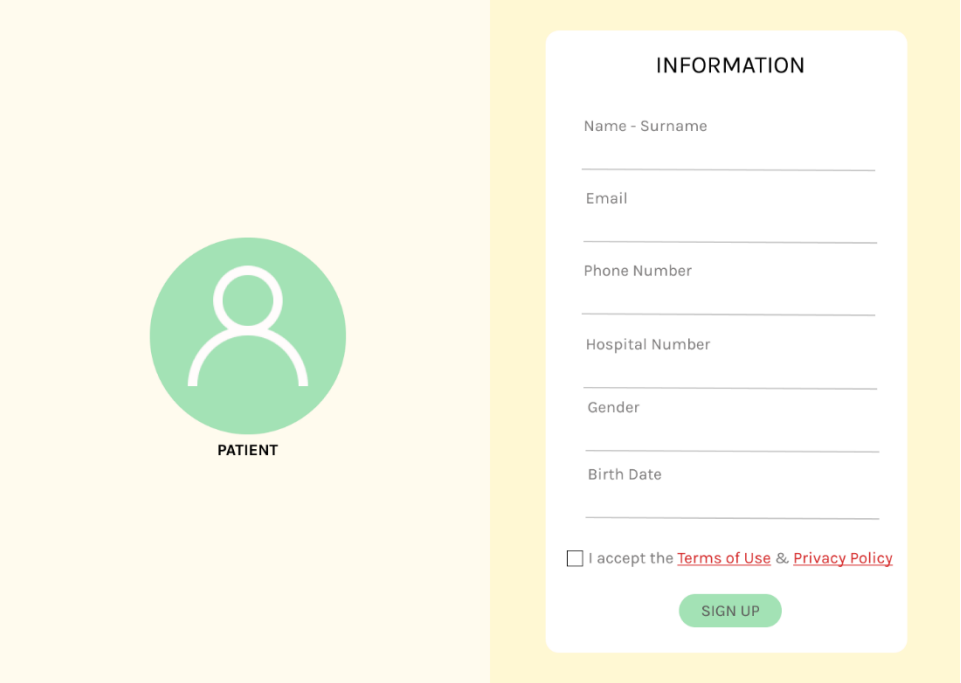


Figure 3.15: Patient role sign-up information page

This page is a page for the patient. In this page, the patient will be able to grant access to the doctor. The patient will be able to choose the hospital that the patient wants to share the data with. Moreover, the patient will be able to choose the doctor that they want to share the data with as well as the rights to the data as shown in Figure 3.11.

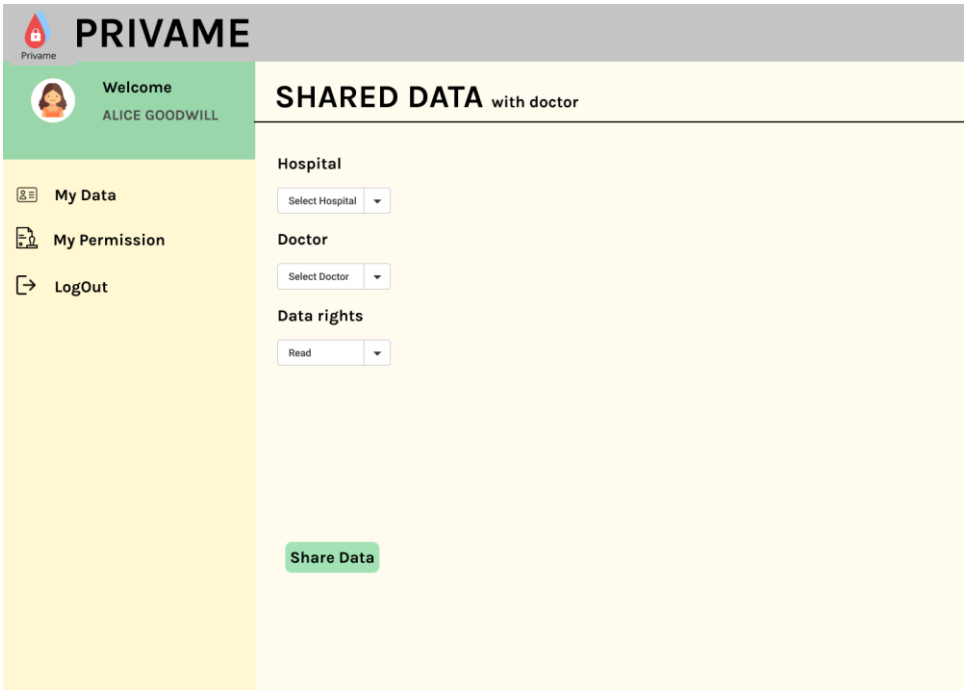


Figure 3.16: Patient access granting page

This is a page for the patient. Patients will be able to see all the access that the patient has granted including the doctor's name, the rights and the filename. The filename could be a transaction of PHR-ID, where PHR stands for Physical Health Record as shown in Figure 4.20.

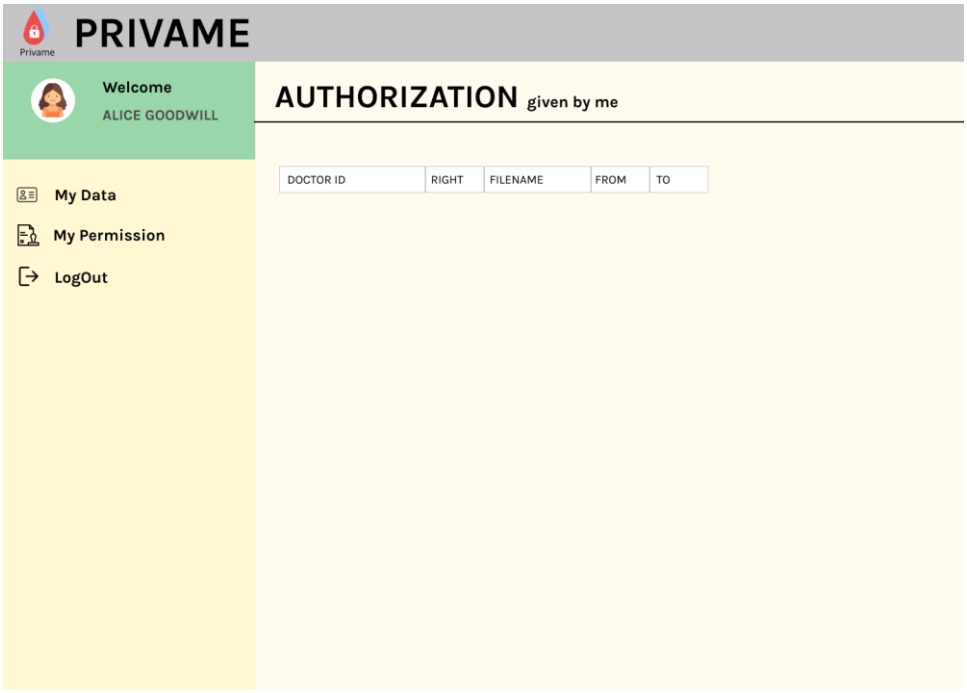


Figure 3.17: Patient permission summary page

This is a page for the doctor. In this page the doctor will be able to see all the access that has been granted by the patient. The doctor will also be able to view the comment and add comments. Moreover, they could download the file as well as shown in Figure 4.21.

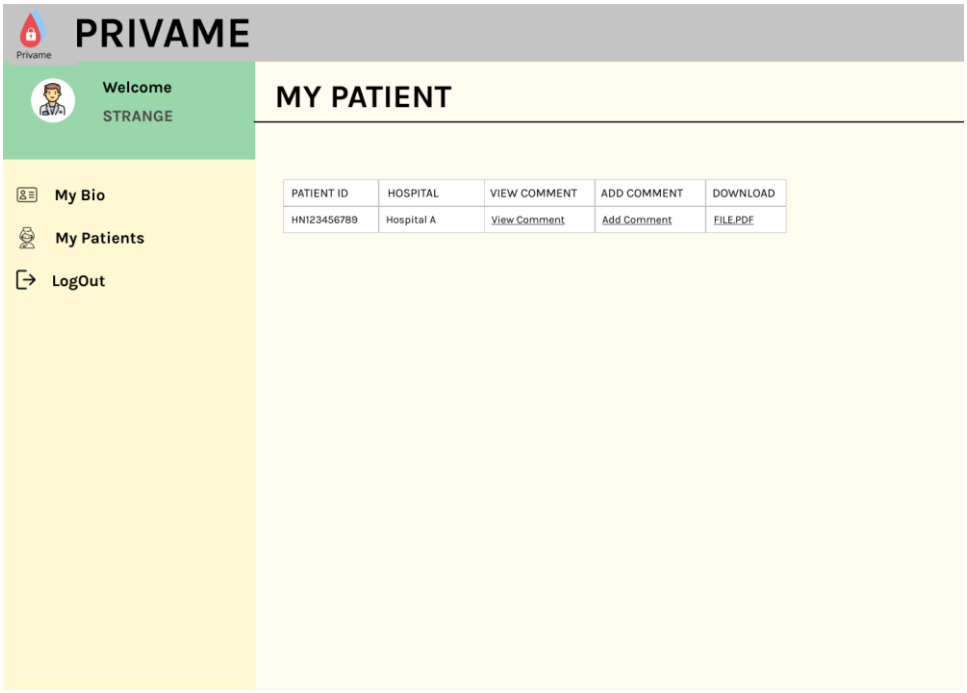


Figure 3.18: Doctor permission grant by patient page

REFERENCES

[1] C. Lei, Y. Ji-Jiang, W. Qing and N. Yu, "A Framework for Privacy-Preserving Healthcare Data Sharing," *2012 IEEE 14th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 341-346, 2012.

[2] S. Yang, J. Rong, Q. Zhenwei and X. Yang, "A Framework of Access Control Model Based on Cross-entropy in Health Information System," *2019 IEEE International Conference on Computer Science and Educational Informatization (CSEI)*, pp. 153-156, 2019.

[3] M. F. F. Khan and K. Sakamura, "A secure and flexible e-Health access control system with provisions for emergency access overrides and delegation of access privileges," *2016 18th International Conference on Advanced Communication Technology (ICACT)*, pp. 541-546, 2016.

[4] A. Dubovitskaya, F. Baig, Z. Xu, R. Shukla, P. S. Zambani, A. Swaminathan, M. M. Jahangir, K. Chowdhry, R. Lachhani, N. Idnani, M. Schumacher, K. Aberer, S. D. Stoller, S. Ryu and F. Wang, "ACTION-EHR: Patient-Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care," *JMIR Publications*, vol. 22, no. 8, p. e13598, 2020.

[5] M. Staffa, L. Sgaglione, G. Mazzeo, L. Coppolino, S. D'Antonio, L. Romano, E. Gelenbe, O. Stan, S. Carpov, E. Grivas, P. Campegiani, L. Castaldo, K. Votis, V. Koutkias and I. Komnios, "An OpenNCP-based Solution for Secure eHealth Data Exchange," *Sciencedirect*, vol. 116, pp. 65-85, 2018.

[6] Shangping, W. Shangping, Z. Dan and Z. Yaing, "Blockchain-Based Personal Health Records Sharing Scheme With Data Integrity Verifiable," *IEEE Access*, vol. 7, pp. 102887-102901, 2019.

[7] "SCB," [Online]. Available: https://www.scb.co.th/th/personal-banking/stories/tips-for-you/pdpa-about-us.html. [Accessed 15 11 2020].

[8] "SCB," [Online]. Available: https://www.scb.co.th/th/personal-banking/stories/tips-for-you/pdpa-rights.html. [Accessed 15 11 2020].

[9] "THE ECONOMIC TIMES," [Online]. Available: https://economictimes.indiatimes.com/definition/authentication. [Accessed 16 11 2020].

[10] "Cambridge Dictionary," [Online]. Available: https://dictionary.cambridge.org/dictionary/english/authorization. [Accessed 16 11 2020].

[11] "vigilance The biopharma PV Specialists," [Online]. Available: https://www.qvigilance.com/what-is-medical-information. [Accessed 15 11 2020].

[12] B. Amit, B. Deepika, I. Nageshwar and I. Meenakshi, "Management of Medical Records: Facts and Figures for Surgeons," *Springer-Verlag*, vol. 10, no. 3, pp. 199-202, 2011.

[13] "Law Insider," [Online]. Available: https://www.lawinsider.com/dictionary/medical-staff. [Accessed 15 11 2020].

[14] R. Bhavani, "Medium," 2019. [Online]. Available: https://bhavaniravi.com/blog/authentication-in-python. [Accessed 15 11 2020].

[15] R. Margaret, "SearchSecurity," May 2018. [Online]. Available: https://searchsecurity.techtarget.com/definition/authentication. [Accessed 15 November 2020].

[16] T. Abi Tyas, "UpGuard," 2 October 2020. [Online]. Available: https://www.upguard.com/blog/sensitive-data#:~:text=Sensitive%20data%20is%20information%20that,unauthorized%20disclosure%20and%20data%20breaches. [Accessed 15 November 2020].

[17] "Cisco," [Online]. Available: https://www.cisco.com/assets/sol/sb/Switches_Emulators_v2_3_5_xx/help/350_550/index.html#page/tesla_350_550_olh%2Fssd_manage.html%23ww1170972. [Accessed 15 November 2020].

[18] EyePornnipa, "PHPBB forum software," 11 September 2019. [Online]. Available: https://www.mindphp.com/forums/viewtopic.php?f=79&t=60368. [Accessed 15 November 2020].

[19] "MariaDB," [Online]. Available: https://mariadb.com/kb/en/about-mariadb-software/. [Accessed 15 November 2020].

[20] S. Ravi, "TecMint," 25 August 2020. [Online]. Available: https://www.tecmint.com/what-is-mariadb-how-does-mariadb-work/. [Accessed 15 November 2020].

[21] "OneLogin," [Online]. Available: https://www.onelogin.com/learn/how-single-sign-on-works. [Accessed 15 November 2020].

[22] W. Yvonne and H. Abhishek, Solving Identity Management In Modern Applications-Demystifying OAuth 2.0, OpenID Connect, And SAML 2.0-Apress (2019), New York: Apress, 2019.

[23] "OpenID," [Online]. Available: https://openid.net/connect/. [Accessed 15 November 2020].

[24] "QA Stack," [Online]. Available: https://qastack.in.th/programming/7699200/what-is-the-difference-between-openid-and-saml. [Accessed 11 November 2020].

[25] "Auth0," [Online]. Available: https://auth0.com/docs/protocols/protocol-oauth2. [Accessed 11 November 2020].

[26] "SSH.COM," [Online]. Available: https://www.ssh.com/pki/#:~:text=Public%20Key%20Infrastructure%20(PKI)%20is,a%20particular%20user%20or%20device. [Accessed 11 November 2020].

[27] "Tutorialspoint," [Online]. Available: https://www.tutorialspoint.com/nodejs/nodejs_introduction.htm. [Accessed 11 November 2020].

[28] "React," [Online]. Available: https://reactjs.org/tutorial/tutorial.html#what-is-react. [Accessed 11 November 2020].

[29] "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/React_(web_framework). [Accessed 11 November 2020].

[30] "Firebase Google," [Online]. Available: https://firebase.google.com/docs/auth#:~:text=Firebase%20Authentication%20p

rovides%20backend%20services,Facebook%20and%20Twitter%2C%20and%20more. [Accessed 11 November 2020].

[31] Jirawatee, "medium," 21 July 2016. [Online]. Available: https://medium.com/firebasethailand/%E0%B8%A3%E0%B8%B9%E0%B9%89%E0%B8%88%E0%B8%B1%E0%B8%81-firebase-authentication-%E0%B8%95%E0%B8%B1%E0%B9%89%E0%B8%87%E0%B9%81%E0%B8%95%E0%B9%88-zero-%E0%B8%88%E0%B8%99%E0%B9%80%E0%B8%9B%E0%B9%87%E0%B8%99-hero-7dd5839d358. [Accessed 11 November 2020].

[32] "mindphp.com," 25 April 2017. [Online]. Available: https://www.mindphp.com/%E0%B8%84%E0%B8%B9%E0%B9%88%E0%B8%A1%E0%B8%B7%E0%B8%AD/73-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3/3872-what-is-postgresql.html. [Accessed 11 November 2020].

[33] S. Montha, "medium," 21 June 2018. [Online]. Available: https://medium.com/@iamgique/postgresql-vs-mysql-13043e4ed2a2. [Accessed 11 November 2020].

[34] "OpenID," [Online]. Available: https://openid.net/connect/. [Accessed 15 November 2020].

BIOGRAPHIES

NAME	Miss Chidchanok Bunjongpean
DATE OF BIRTH	15 April 1999
PLACE OF BIRTH	Samut Prakan, Thailand
INSTITUTIONS ATTENDED	Matthayom Watnairong School, 2017: High School Diploma Mahidol University, 2020 : Bachelor of Science (ICT)

NAME	Miss Ariza Dolsooklert
DATE OF BIRTH	12 November 1998
PLACE OF BIRTH	Bangkok, Thailand
INSTITUTIONS ATTENDED	Potisarn Pittayakorn School, 2017: High School Diploma Mahidol University, 2020 : Bachelor of Science (ICT)

NAME	Mr. Jiraput Thamsongkrah
DATE OF BIRTH	12 July 1998
PLACE OF BIRTH	Bangkok, Thailand
INSTITUTIONS ATTENDED	Suankularb Wittayalai Nonthaburi School, 2017: High School Diploma Mahidol University, 2020 : Bachelor of Science (ICT)