Runar Moen
Abdurahman Godana

Bachelor's thesis

Negotiating Privacy Settings in Homecare through Android Applications

May 2022

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Design

NTNU
Norwegian University of
Science and Technology

Bachelor's thesis

2022

NTNU
Norwegian University of
Science and Technology

Runar Moen
Abdurahman Godana

Negotiating Privacy Settings in Homecare through Android Applications

Bachelor's thesis
May 2022

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Design

NTNU
Norwegian University of
Science and Technology

Negotiating Privacy Settings in Homecare through Android Applications

Runar Moen, Abdurahman Godana
Digital infrastructure and Cybersecurity at NTNU, Gjøvik

Abstract

From 2019 to 2021, the use of e-health services here in Norway has increased by 13%[1]. This has of course brought many benefits, but also raises some privacy issues for both patients and the caregivers who care for them. This could be a concern, especially in scenarios where there are conflicts between patient privacy and the demands on caregivers to do their jobs. For example, if a patient is placed in a nursing home, when should the caregiver have access to their room? Is there perhaps a way to handle this electronically without causing either party a lot of stress? And what information should be disclosed to the other party when it comes to maintaining privacy between patient and caregiver? These were the main concerns we wanted to address in our thesis.

During the project, we developed a proof-of-concept software agent that allows both patients and caregivers to manage and synchronize their privacy settings simply and securely. The software consists of an Android application running on the client-side and an associated server that we deployed on the NTNU OpenStack network. Throughout the project, we applied the Design Science research methodology with a focus on extending and improving the application in the future.

We conducted a study regarding privacy in-home care to gain insight into the development process. First, to support the study, a questionnaire was developed and distributed to three different user roles: patients, caregivers, and patient's family members. The results of the survey conducted served as the basis for determining the privacy settings to be implemented in the software.

In this paper, we discuss both the technical aspects (related to the development of the software) and the research aspects (related to the implementation of the survey) of our project and provide some insight into what we think might be a good solution to the questions posed above. We also discuss the shortcomings of our project and the aspects that we believe could be improved if we were to evolve the application from a proof-of-concept to a finished product.

Sammendrag

Fra 2019 til 2021 har bruken av e-helsetjenester her i Norge økt med 13%. Dette har selvfølgelig fulgt med mange fordeler, men bringer også noen personvernspørsmål for både pasienter og omsorgspersonene som jobber dem. Dette kan være en grunn til bekymring, spesielt i tilfeller der det er konflikt mellom pasientens personvern og kravene som stilles for at omsorgspersonen kan gjøre jobben sin. Hvis en pasient for eksempel sitter i et sykehjem, når skal omsorgspersonen få tilgang til rommet deres? Er det kanskje en måte å håndtere dette elektronisk uten å påføre noen av partene stress? Og hvilken informasjon bør motparten ha tilgang til når det skal det er spørsmål om å opprettholde personvernet deres. Dette var problemstillingen vi ønsket å diskutere i oppgaven vår.

I løpet av prosjektet utviklet vi et konseptbevis på en programvareagent som lar både pasienter og omsorgspersoner kontrollere og synkronisere personverninnstillingene sine på en enkel og sikker måte. Programvaren består av en Android klient og en tilhørende server som vi distribuerte på NTNU sitt OpenStack-nettverk. Gjennom hele prosjektet brukte vi Design Science forskningsmetodikken med et fokus på å utvide og forbedre applikasjonen i fremtiden.

Vi gjennomførte også et studie om personvern i sykehjem for å få innsikt i hvordan vi skulle gjennomføre utviklingsprosessen. Dette studiet inkluderer en spørreundersøkelse fordelt på tre ulike brukerroller: pasienter, omsorgspersoner og pasientens familiemedlemmer. Resultatene av dette studiet ble brukt som grunnlag for å bestemme hvilke personverninnstillinger som skulle implementeres i programvaren vår.

I denne oppgaven har vi diskutert både de tekniske (relatert til utviklingen av applikasjonen) og forskningsrelaterte (relatert til spørreundersøkelsen) aspektene av prosjektet vårt og gir innsikt i hva vi mener kan være en god løsning på spørsmålene ovenfor. Vi vil også diskutere det manglende ved prosjektet vårt og de aspektene som vi mener kan forbedres hvis vi skulle ta programvaren fra et konseptbevis til et ferdig produkt.

Preface

We would like to thank our provided advisor, Guoqiang Li for his continuous support throughout the project. He has provided us with both insight into writing the report and designing the software. We would also like to thank Luyi Sun for her help throughout various aspects of the project, especially with her help in performing the research study and being available for guidance whenever we needed; Pankaj Khatiwada for helping us with technical aspects and looking into getting us API access for the electronic door lock; and of course, Bian Yang for letting us do this thesis, and taking his time to provide regular feedback whenever it was needed. We would not have been able to complete this study without your continuous support.

Acronyms

ACID Atomic Consistent Isolation Durability.

API Application Programming Interface.

DNS Domain Name System.

DSR Design Science Research.

eHWS eHealth and Welfare Security.

GC Yao's Garbled Circuit.

GDPR General Data Protection Regulation.

GW Gateway.

HTTP Hypertext Transfer Protocol.

IND-CCA Indistinguishability under chosen ciphertext attack.

JDK Java Development Kit.

JRE Java Runtime Environment.

JVM Java Virtual Machine.

NTNU Norwegian University of Science and Technology.

OWASP Open Web Application Security Project.

SDLC Software Development Life Cycle.

SQL Structured Query Language.

SSL Secure Sockets Layer.

TCP Transmission Control Protocol.

UDP User Datagram Protocol.

UML Unified Modeling Language.

WPAN Wireless personal area network.

Contents

Figures

Chapter 1

Introduction

1.1 Thesis Background

In recent years, there's been a major shift towards electronic health services in Norway. During a yearly study performed by the Norwegian Directorate of eHealth, it was reported that the number of people using electronic health services has increased from 33% in 2019 to 46% in 2021 [1]. While these services can be greatly beneficial to the general populace, it does raise some interesting security questions. Especially in regards to the privacy of patients and caregivers.

This project work primarily addresses patient privacy in the context of home care monitoring systems or assistive living technologies. To use software agents to improve privacy in-home care, we consider and describe in detail different scenarios such as electronic door locks or the installation and configuration of cameras in the home of patients living in health care centers. The scenarios are supported by the development of a prototype Android application that allows easy management of privacy settings without requiring the user to have a technical background. By doing this, we hope to facilitate communication between multiple parties and establish agreements on privacy settings.

1.2 Research Question

In this thesis we intend to address the following research questions:

- How can the different privacy preferences of individual user roles be addressed in-home care?
- How can we synchronize the privacy settings of different user roles in a home care environment?
- What technologies or tools can be used to enable negotiation in the software agent being developed?

This paper is about figuring out how best to address the privacy preferences of individual patients by providing a relevant questionnaire about different

scenarios (such as electronic door locks, camera recordings, or other monitoring technologies) and synchronizing the conflicts that arise during communication between multiple parties to reach an agreement on privacy settings using the developed Android application.

1.2.1 The Problem Statement

The aging population in Norway has been increasing dramatically recently. In 2021, it has already reached one million, the highest number ever recorded[2]. The use of monitoring systems and assistive technologies has been introduced to make life easier for older people living in-home care, and this technology has many benefits. For example, the use of these assistive technologies can reduce health care spending by introducing automation. The research and industry projects that have been conducted so far help patients and elderly people to more comfortably live at home. The introduction of new technologies and systems comes with some security constraints when it comes to individual privacy preferences. For example, if a caregiver plans to visit the patient with an electronic door lock and it's automatically unlocked without considering the patient's will, it may affect the patient's privacy. The focus of this work is to allow nurses and technical staff working with patients to consider the privacy preferences of each individual patient. We have developed a software agent that allows us to synchronize privacy settings and performed a small-scale study with different scenarios where the patient's and privacy might be compromised.

1.2.2 Boundaries

We must establish the boundaries of our project to ensure there are no misunderstandings. First of all, our software is simply intended as a proof of concept. This means that there are going to be key features that one might be used to seeing in other applications (e.g language settings, password recovery, notifications) that could be missing. We have primarily focused on the privacy setting and negotiation aspects of the software. It is also important to note that the software agent is compatible with Android devices only. While it's definitively a possibility to port it to other devices, we're unfortunately unable to do so now because of time constraints.

When it comes to the study, it is important to keep in mind that it was a small-scale study with only a total of 8 users. We were also unfortunately not able to have actual patients (or family members of patients) answer the study. Instead, we had acquaintances of us answer the study in their place. And although they were not real patients, they were asked to answer truthfully about what they would do if they found themselves in that position.

1.2.3 Motivation

One of our main motivations is a concern for the privacy of patients using electronic devices. We believe that it is very important to establish a proper infrastructure to help manage their privacy when using these assistive technologies and monitoring systems. This is especially true when they are in their home care centers, where they might feel their privacy is comprised. Despite this, we also believe it is important to allow the caregivers to perform their job. We hope that by developing this system, we can remove some of the stress on both patients and caregivers by negotiating their privacy input for them, based on their input. This information could also be very helpful for our employer NTNU, and their eHealth and Welfare Security research group.

1.3 Workload

In this section, we will talk a little bit about how we've distributed the workload among our group. As this was a large project that covers a wide variety of tasks, we decided it was important to distinguish our roles early on. **Runar Moen**

- Responsible for planning and developing the majority of the software
- Acts as a contact person for third parties.
- Responsible for quality control for reports or other documents.
- Quality control for grammatical or spelling errors in reports.

Abdurahman Godana

- Responsible for planning and performing the research components
- Responsible for archiving documents and submissions.
- Organize and suggest appropriate times for meetings.
- Ensure all files produced are well documented and stored in the correct location.

1.3.1 About us

We are a group of two members, both students at NTNU in Gjøvik studying the same degree, Bachelor in Digital Infrastructure and Cyber Security. Before this project, we had a lot of experience that would be useful, including (but not limited to) knowledge of software engineering, networking, programming, and databases. While these experiences certainly helped, there was still a lot we had to learn. Thankfully, this project provided us with a great outlet to expand on our knowledge, which we are extremely grateful for.

Chapter 2

Research Methodologies

We have divided our work into a research part and a software development part. In the research part, we mainly focus on investigating whether privacy-enhancing technologies can protect patient privacy through software-based negotiation of privacy settings. To support this idea, we planned a survey on different users in real life which would form the basis of the settings used in our software. The second part is to design an application that will serve as a software agent for healthcare providers and patients to communicate with each other and make agreements about privacy preferences. For this, we chose to design an Android app following the Scrum frameworks in Software Development Life Cycle (SDLC), an agile development methodology based on an incremental and iterative process for software development[3]. Scrum is a fast, flexible, adaptable, and effective agile model developed to add value to the customer in the development process. The goal of Scrum is to meet the needs of the customer through smooth communication and continuous progress.

2.1 Scientific methodological approach

As a basis for our research, we used Design Science research methodology[4]. DSR seeks to enhance technology and science knowledge via the creation of innovative artifacts that solve problems and improve the environment in which they are instantiated[4]. The DSR process is a widely used research paradigm proposed by Peffers, Tuuanen, Rothenberg and Chatterjee in 2008. It is commonly used in development projects like ours.

The main objective of the Design Science research methodology is to obtain knowledge through the creation of artifacts. In the context of our project, the artifact would be our software. Developing our software does not only serve to create a product but also helps to gain insight into the problem area by evaluating it. By doing this we can gain a better understanding that can be used for future projects and improve upon what we've built. This "build-and-evaluate loop" is one of the main principles of the Design Science model[**design-science**]. We used the following 6 steps with the methodology.

- Problem identification and motivation:
- Definition of objectives for a solution
- Design and development
- Demonstration
- Evaluation,
- Communication.

Secondary data sources were primarily used to investigate standard implementation solutions and development schemes. Due to the constant updates that technologies now rely on [5], it was necessary to use the Internet as a source for vendor documentation, articles, and videos. Additionally, we collected relevant information[6] and personal insights on how modern care homes are working. An unstructured conversation was conducted with Luyi Sun, a doctoral student at NTNU. The unstructured conversation provided an opportunity for ongoing conversations either in person or via online communication services.

2.2 Information Gathering

2.2.1 Vendor Documentation

Vendor documentation was used extensively during the development of the application. For example, the Android developer guidelines were used in setting up Android Studio and learning the unique Android-specific syntaxes. We made sure to do research on the majority of the technologies used, including (but not limited to) the database platform, the IDEs, and the OS of the server. These were all taken directly from the vendor's website, to ensure it's up to date and contains the proper information.

2.2.2 Questionnaire

In this section, we will describe the methods used to gather information for our study. First, we collected the research questions and divided or grouped them into different scenario categories, namely electronic door locks, cameras, other surveillance technologies, and incident-related scenarios. The questions were made for three user roles. Patients, caregivers, and family members. We mainly focused on the patient and caregiver roles, as they were the ones we had planned to implement. The family role was something we intended to implement if we had enough time.

The questionnaire consisted of 15 questions for the patient and the caregiver and an additional 10 questions. We sent a proposal to three care centers and contacted them by phone and email in hopes of performing the study with them. Unfortunately, after the discussions were conducted, the managers or administrators did not let us proceed to conduct the planned interviews and questionnaires, after which we ended up looking for another option.

We managed to find a small nursing home in the same municipality of Gjøvik where patients of young age with different types of disabilities lived. In the first round of this data collection. After consultation with the administrator, we decided to invite 7 participants from this home. We decided to divide them into three small groups. The first group consists of 3 caregivers, the second group consists of 2 patients, and the third group consists of 2 parents of patients. For the first user role, caregivers, we distribute the questionnaires by email after giving them a brief introduction to the topics and gaining their consent. The caregivers successfully answered the distributed questionnaire, but for the other user roles, especially the patients with whom we wanted to conduct an interview, this was not possible because the administration told us that the patients could not provide sufficient consent. This meant we could not conduct an interview or questionnaire with the second and third user roles. To find a solution, we contacted some of our friends, including our families, to participate in the interview and questionnaire where they would assume they were in the position of a patient or their parents. This solution ended up working and we successfully conducted data collection using the questionnaire for the remaining two user roles. The process of data collection was not easy, but finally, we managed to collect all the planned surveys with different user roles. .

Chapter 3

Requirement Analysis

In the previous sections, the introduction and scientific methodologies were presented. The report also includes the requirements analysis phase, so this section will describe this particular phase in-depth and provide a detailed description and definition of the requirements.

3.1 Requirements Specification

Well defined requirements are important for the success of the project. They create a structural agreement between the customer and the service provider to achieve the same goal. Requirements creation is a complex task consisting of analysis, specification, validation and management. In this section, we will discuss the types of requirements for our software agent products and provide a set of recommendations for their use.

3.1.1 User Requirements

Our employers (NTNU) expectations have been specified and are clearly defined. They are outlined in a user requirements specification and includes understanding user requirements through survey and interviews with (patients, caregivers, and family members), and building an Android mobile app based on feedback from user requirements. And finally, synchronizing patient and caregiver privacy settings in different scenarios using a software agent. To help meet these expectations, we've separated the functional and non-functional requirements of the application.

3.1.2 Functional Requirements

The Functional Requirements are the product features or functions we should implement to accomplish our tasks. It describes the system behavior under specific conditions. For example, the system sends authentication for the users to log in. Here are some of the functional requirements of our application:

- Registration
- Authentication
- Configuration of privacy settings
- Synchronization of privacy settings
- User roles (patient, caregiver)
- Compliance to laws or regulations

Nonfunctional Requirements

Nonfunctional requirement describes how the system behaves and establishes constraints of its functionality rather than defining how the system performs [7]. In contrast to the functional requirements, this mostly focuses on user expectations. In the context of our project, this includes the scalability, usability, and performance of the system.

3.1.3 Use Case Diagram

In this section, we will explain our Use Case diagram to help give an understanding of the various user requirements. Here we define an actor as someone who uses the home care app system to achieve their goals. This can be a caregiver, visitors (nurses, physical therapists, the community, families), or other systems or organizations. The most common actors downloading our home care app are caregivers. These actors should always be considered as external objects, which is why we place them outside the system. The other actors should be categorized as a specific person or organization. In our context, caregivers can be considered as main actors. The function of the main actor is to initiate the use of the system. They open the home care app and do something like synchronizing the patient's privacy, locking/unlocking the electronic door lock, setting/configuring the camera, setting personal data and ... etc..

Another actor in our diagram is the patient. The figure below describes the system and how they interact in more detail (see figure 3.1).

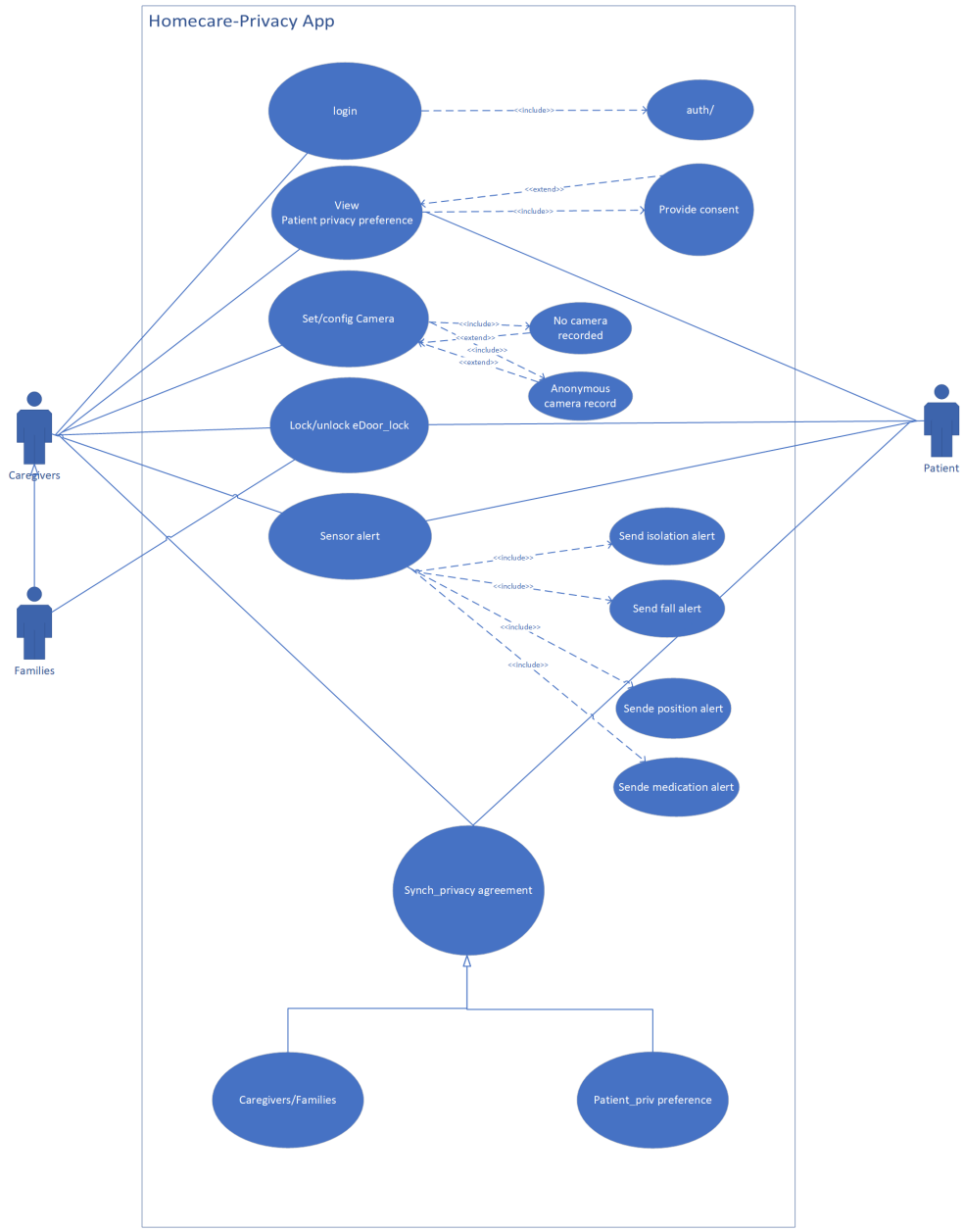


Figure 3.1: Use Case diagram for the application

As we mentioned, the actor is the one who uses the system to achieve the desired goals. Thus, each actor interacts with one of the use cases within the system. A use case represents an action that performs some kind of task within the system. They are represented as the oval shapes in the diagram. There are four types of relationships in the system: association, inclusion, extension, and generalization. The association relationship is represented by a solid line that connects actors to a type of task or action in the system or connects actors to a

use case. A caregiver also interacts with the other use cases using the solid association line. Typically, each actor must interact with at least one use case. The secondary actors, i.e., the patient, can also be involved in the use cases, in particular, the patient privacy use case, the electronic door lock, the sensor alarm, and the synchronizing privacy agreement.

If the caregiver wants to visit, they must negotiate and follow the privacy settings and make an agreement. We use an include relationship to define the dependency between a base use case (e.g. login, set camera, electronic door lock, and sensor alert) and an include use case (e.g. authentication , camera records, anonymous camera records, send isolation alerts, send fall alerts). Each time the base use case is executed, the included use case is also executed. The base use case requires an included use case to be completed. For an include relationship, we used a dashed line with an arrow pointing to the base use case.

An extension relationship has a base use case and an extension use case. When the base use case is executed, the extension use case is sometimes executed, but not always. The extended use case occurs only when certain criteria are met. An extended relationship is represented by the dashed arrows pointing to the base use case. The difference between the include and extend relationship is that the include relationship always occurs, while the extend relationship only occurs sometimes and the arrows point in the opposite direction. Another type of relationship is a generalization, for example, if the caregiver sees or considers the patient's privacy preferences during his visit and on the other hand, the patient's privacy preferences are protected. Then the negotiation is determined by synchronizing the privacy preferences of both parties.

3.1.4 Application flowcharts

Application flowchart description

This figure (3.2) The application flowchart is a graphical representation that shows the steps required during the application. It is used to visualize the sequence of steps that must be followed in the project management process from start to finish. For example, once the caregiver opens the home care app and logs in, the authentication process begins. If he does not have an account yet, he registers and is authorized for the login process. If he already has an account, he goes directly to the main menu. Then he selects the type of service he wants to provide, and then checks the patient's privacy settings to lock or unlock the electronic door lock, depending on the task. If both parties, i.e. caregiver and patient, agree with their privacy settings, the agreement is synchronized and the required tasks are performed.

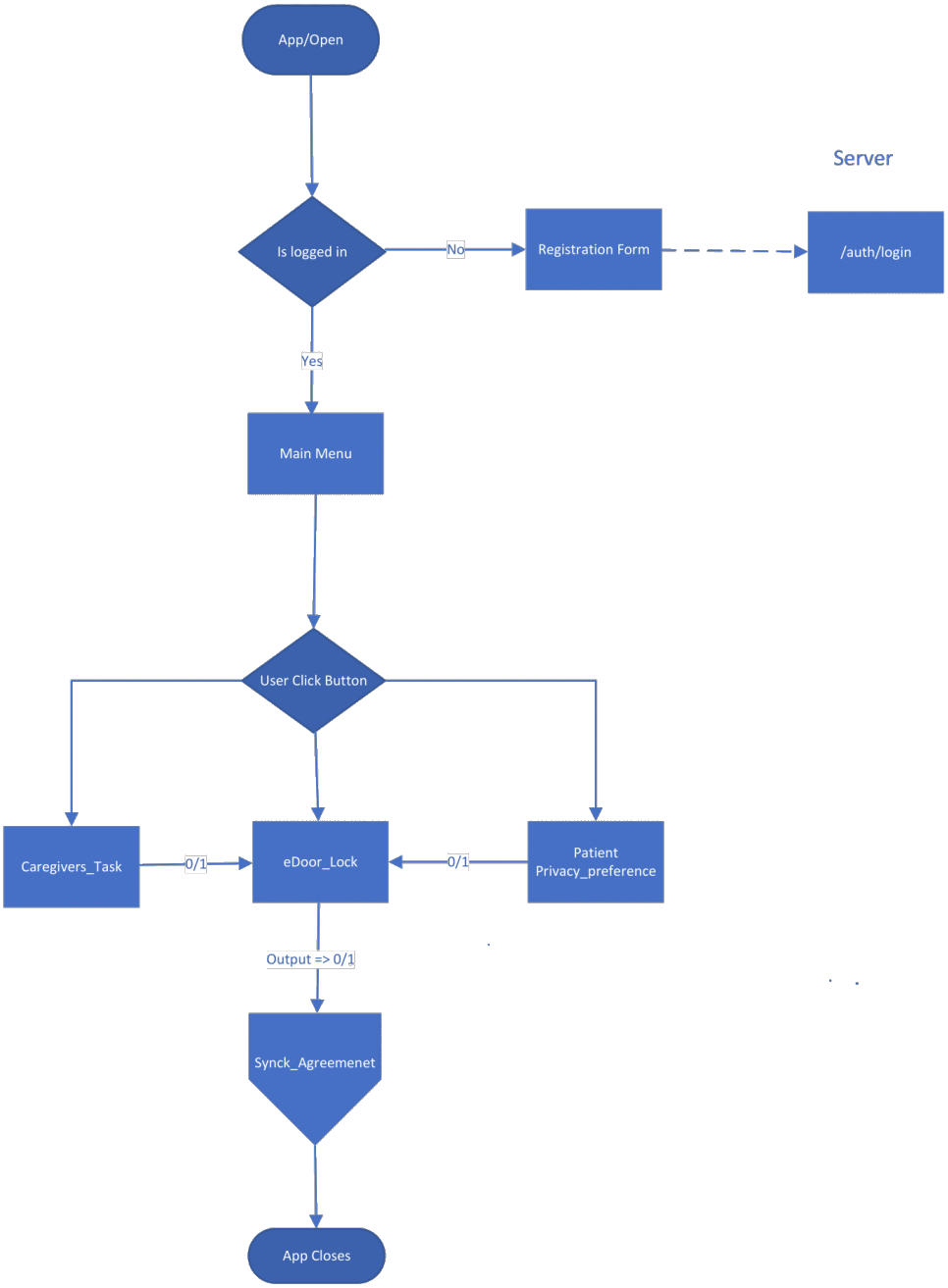


Figure 3.2: Application flowchart

3.1.5 User stories

User Stories are short explanations and descriptions of what needs to be done from the perspective of the partner/user who wants to achieve that functionality or result.

```
As a "Role/User" I want to "Functionality" so that "Benefit".
```

Based on the above Formula, we defined the following user stories:

```
As a developer, we want to design an Android app that serves as a
software agent and deals with patient privacy scenarios so that
healthcare providers and patients can communicate and make
agreements about privacy settings.

Since we are designing an app, we would like to create a
negotiation logic that deals with patient privacy scenarios
so that users can easily synchronize an agreement when using the app.
```

3.1.6 Product Backlog

A product backlog is an ordered list of everything known to be needed for the product. A prioritized list of product features that drives stakeholders to turn their vision into a working detail. In our case, it is a list of activities in our application for improving patient privacy in nursing homes. Product backlog is the single source of requirements needed for all changes to the product. The Product Owner is responsible for the Product Backlog, including its content, availability, and arrangement. The Product Backlog does not focus so much on what the team will do in the distant future, but gives higher priority to things that need to be done in the near future. Due to the evolving nature of the Product Backlog. The assumption is that requirements and conditions will continue to change in the future, so the focus is on the things that are most likely to happen. The higher priority items are at the top of the list and again the duration of sprint is kept from week one up to four week's. The lower priority items at the bottom of the list. See table 3.1

	PRODUCT BACKLOG					
NO	As a...	I want to be able to...	So that...	Priority	Sprint	Status
1	Caregivers	Login to the home-care application via my phone	I can take a look at activity lists	Must	1	Done
2	Caregiver	look at each patient's privacy preferences as I plan to deliver care	I can consider patients' privacy concerns to avoid compromising their privacy	Must	1	In progress

Table 3.1 continued from previous page

3	Caregiver	set up camera surveillance when the situation permits and after consulting with them	I can set up remote communication to increase the safety of elderly people in their room.	Could	1	In progress
4	Caregiver	grant visitors access permission to lock or unlock the electronic door lock.	I can keep entryways secure.	Could	1	In progress
5	Caregiver	establishing sensor alarm technologies at nursing home.	I can monitor the daily mobility of patients living alone in their nursing home.	Should	1	To be done
6	Patient	not allowed to install camera recordings in my room due to my health impairment	I have control over my personal privacy.	should	1	To be done
7	Patient	accept anonymous camera recordings due to my health deterioration.	I receive the necessary help in time in case of unexpected incidents.	Must	1	To be done
8	Patient	Give consent if I want to or if my state of health does not allow me to carry out my daily activity.	I can afford the necessary assistance and help from the care provider.	Could	2	To be done
9	patient	Have the sensor alarm turn on automatically when I am exposed to a fall, heart attack or seizure.	I have received an active response and help.	Must	1	To be done
10	Patient	Not accepted as a caregiver, or visitors will automatically unlock the electronic door lock and enter unless iam given permission to do so.	I cannot have my privacy invaded	Must	2	In progress

Table 3.1 continued from previous page

11	Family	visit a patient in his nursing home	I prefer to get permission to open the electronic door myself if I have made an appointment in advance for my visit.	Could	1	In progress
12	Family	not be monitored by an existing surveillance system that monitors all my activities, whether I am in the nursing home or at home.	*It does not invade my privacy*	Must	1	Done

Table 3.1: Home care application Product Backlog

3.2 Data Analysis

The following table shows the responses to the questionnaires we completed. They were separated into three different questionnaires. One for caregivers, one for patients, and one for family members. They were asked a variety of questions. These range from being about door locks, cameras, and even some incident scenarios. We then took the response and determined what the majority agreed on. This was then turned into a value of either 1 or 1, depending on whether they agreed or disagreed with the statement. These were then used in a logical calculation. The output is the calculated result of P C F or P C F , depending on whether it is a logical conjunction (AND) or disjunction (OR). For the majority of statements, we will use logical conjunctions, unless there's a danger to either party, in which case we will use a disjunction.

Note that the role of the family is not included in all scenarios. In this case, it is marked with an "X" in the table and is not included in the negotiation process. In some scenarios, we've also included a variable where certain legal restrictions may apply. This variable overwrites all of the other preferences (which means that if it's 1, the result automatically becomes 1, and vice versa). Note that the family and legal columns are not implemented in the software itself yet, but are present here to show how we can create more complex negotiations by introducing more variables.

In the following table3.2:

- P = 1 means YES I agree with the statement, P = 0 means, NO, I disagree with the statement. For the patient.
- C = 1 means YES I agree with the statement, C = 0 means, NO I disagree with the statement. For the caregivers.
- F = 1 means YES I agree with the statement, F = 0 means, NO I disagree

with the statement. For the family members.

- L = 1, if the constraint of the legal norm is true, means that the decision can override the preferences of all other user roles. For example, the predefined emergency rule would be implemented in case the patient refuses to open the door and is in a life-threatening situation.
- O = 1/0, Shows the result that would be YES/ NO. It is the result that could be calculated with the logical calculation conjunction (AND) or with the logical calculation disjunction (OR).

In the Explanation column, the expected result is described in more detail. See table 3.2

Table 3.2: Logical calculation conjunction(AND) and disjunction(OR) based on caregiver, patient and family input

No's	Statement	AND/OR	C	P	F	L	O	Explanation
Q1	The caregiver is visiting the patient while they are in good health condition, should the caregiver be given access to the door through an electronic door lock?	AND	0	1	X	X	0	Since the patient and caregiver are not in agreement, the caregiver will not receive access to the electronic door lock.
Q2	The patient is visited by his relatives in his room. Should the caregiver gain access to the door and open it for him?	AND	0	0	1	X	0	Since the three users are not in agreement, the caregiver will not receive access to the electronic door lock.
Q3	Physiotherapists visit patient in normal state of health. Should the caregiver be given access to open the door for physiotherapist?	AND	1	1	X	X	1	Since the patient and caregiver agree, the caregiver gains access to the door and can open it for the visitors.
Q4	Caregivers visit patient in normal health but are busy with other things and do not want to be disturbed. Should the caregiver be able to open the door to check up on the patient?	AND	1	0	X	X	0	Since the patient and the caregiver disagree, the caregiver cannot open the door.

Table 3.2 continued from previous page

Q5	The patient is unable to open the door. Does the caregiver use communication mechanisms such as (video call, text message) before opening the door to know his condition beforehand?	AND	0	1	X	X	0	Since the patient and the caregiver disagree with the statement, the caregiver will not be able to open the door.
Q6	The patient is in their room and does not want the caregiver to visit. Should the patient be able to refuse consent?	AND	1	1	X	1	1	Since both the patient and the caregiver agree with the statement, the patient has the right to say that the door shouldn't be opened. Their will should be respected unless they're in danger then the legal requirement should override the decision during emergency.
Q7	The patient is in their room and does not want the caregiver to visit. They are being supervised by their family member. Should the patient be able to refuse consent?	AND	1	1	X	1	1	There is an agreement in between both parties as patient can decide for themselves, if there is conflict then the legal requirement should override the decision during emergency.
Q8	Caregiver comes to see a patient with a serious illness. Should the caregiver be allowed to enter?	OR	1	1	1	X	1	Since either the patient or the caregiver agrees with the statement, the caregiver is granted access to the door to help the patient.

Table 3.2 continued from previous page

Q9	The patient has an alarm that detects incidents (e.g., a fall alarm). If the patient is showering or getting dressed and a serious medical problem suddenly occurs (e.g., a heart attack or seizure), should the alarm automatically notify the caregiver?	OR	1	0	1	X	1	Since either the patient or the caregiver agrees with the statement, the caregiver is automatically notified.
Q10	The fire alarm goes off while the patient is in the nursing home. Should the door open automatically when this happens?	OR	1	1	1	1	1	All parties agree on the life-saving declaration.
Q11	Police arrive after receiving a call from a traumatized patient. Should patients who are not in a normal state speak directly to the police without being disturbed?	AND	1	1	X	X	1	All parties are agreeing with the statement as patients can talk to police directly.
Q12	The patient is suddenly exposed to falling accidents while performing activities such as making the bed or cleaning his room. Could you imagine that there is a mechanism to report incidents?	OR	1	0	1	X	1	At least one of the parties agree that there will be a system or monitoring technologies such as cameras can be activated that will allow patients to inform the centre staff themselves about the incident.
Q13	The patient is suffering from a chronic disease. Should the caregiver be able to check on him personally instead of monitoring tools?	OR	1	0	0	X	1	Since either the patient or the caregiver agrees with the statement, the caregiver is granted access to the door for control purposes.

Table 3.2 continued from previous page

Q14	Should communication devices be used in the patient's room to help with the feeling of isolation?	AND	0	0	X	X	0	Since two of the parties are disagree with the statement, rather they prefer to participate in social engagement activities to reduce feeling of isolation.
Q15	Should the patient's personal data be encrypted and only accessible to them?	AND	1	1	X	1	1	Since both users agree with the statement, the users data will be encrypted and only accessible to them. Even if no agreement in between parties, The Legal norm restriction will apply when the decisions are irrational to prevent the loss.

The following tables show the results of the AND and OR operator being used with two parties.

Table 3.3: Logical table for AND computation

P	C	O
1	1	1
1	0	0
0	1	0
0	0	0

Table 3.4: Logical table for OR computation

P	C	O
1	1	1
1	0	1
0	1	1
0	0	0

3.3 Hypothesis

Once the negotiation process happens, it would protect patients' potential risk and this can be predicted results. If healthcare providers cannot consider patient

privacy while making medical decisions and providing clinical care, it would put patients' lives at risk. so it is very important to set up individuals' privacy settings and behaviors while patients are being monitored at the care home. Both technical staff and health care providers should have to take patients' privacy concerns into account while providing necessary assistants and medical care to the patient. Additionally, having a software agent allowing them to synchronize on privacy settings will help both parties to communicate and make agreements on their privacy settings.

3.4 Electronic Door Lock

Originally we intended to implement an electronic door lock into our application. However, because of time constraints, we were unable to get access to the API in time. In this section, we will describe how we planned to integrate the electronic door lock.

The door lock would be placed in the server, where it would be managed based on the privacy settings provided by the users. The information required to establish a connection with the door lock would be stored in our database. While we are not entirely sure what would be required, it would likely at least contain some identifying information about the owner of the lock, and some sort of authentication towards the lock itself. We would obviously have to ensure proper storage of this data to ensure that the owners personal information is not put at risk and that no bad actor could open the door lock unauthorized. Safe4 - Iotiliti Information security setup - overview.

Chapter 4

Technical design

4.1 Client-server model

Our software is based on the client-server model, which separates the task of the software into two main components, the client which is installed on the phone of the user, and the server which is running on a virtual machine in the cloud. There is also a database component, that handles the storage of data.

4.1.1 Client

The client is the Android application that runs on users' phones. It is compatible with Android 11 and above. The client's primary role is to process user input, display output to the user, and connect to the server. The client displays the various privacy settings and allows the user to enable or disable them.

4.1.2 Server

The server is the component that processes most of the logic in our system. It constantly waits for a user to connect and then performs the tasks that the client needs. Each client is processed in a separate thread on the server, so it can perform multiple user tasks synchronously. The server is responsible for the negotiation part and deciding whose privacy preference should take precedence. Since most of the logic is handled by the server, this allows for both horizontal scaling with load balancers and vertical scaling by improving server specifications.

4.1.3 Sequence Diagram

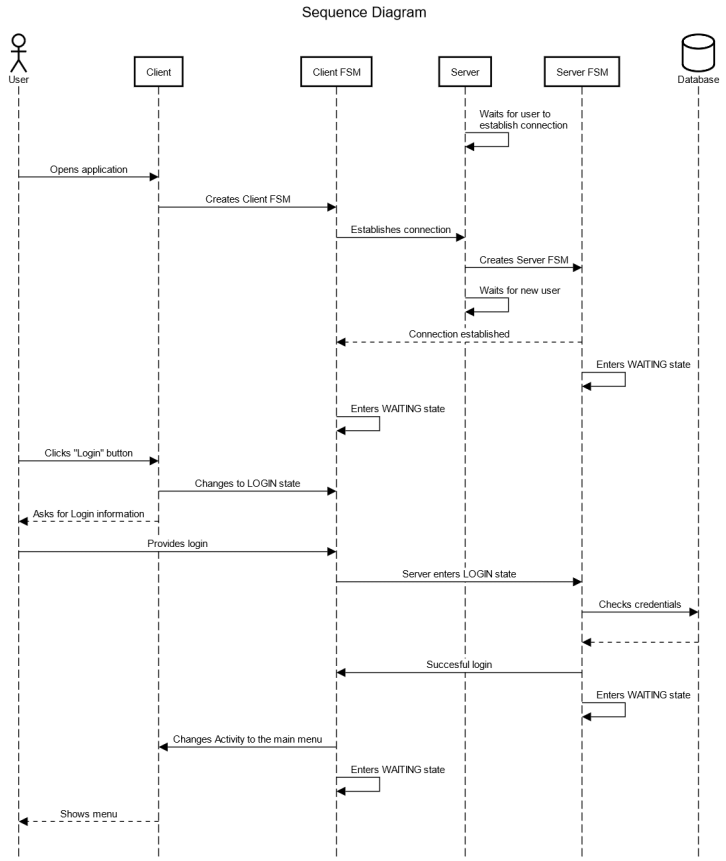


Figure 4.1: Sequence Diagram

The following Sequence Diagram describes how the various parts of the software interact with each other. The user opens the application, which causes the client to create a new thread with running parallel with the android activities. In this thread, there's a Finite State Machine constantly waiting for an update in the main thread. Once the state machine is created, it will attempt to establish a connection with the server. After the user performs any action that would change the software state (e.g. attempt to log in), the state machine would perform the appropriate action in the background.

4.2 Negotiation

The negotiation process is where the patient and the caregiver's privacy settings are synchronized. Before the process begins, both users answer a questionnaire with regards to their privacy settings, this questionnaire is based on the survey discussed in the previous chapter (see table 3.2). Once the users have answered

the questions, they will be able to start the negotiation process. Each question is either All the input of the users will be stored in an encrypted string, which is decrypted for the negotiation. The software takes the decrypted strings, compares them, and stores the new value. The following table 4.1 is an example of how the negotiation process works. Here, we take the string of user inputs and separate them into Boolean arrays, we also have another array that decides whether it's a conjunction (A) or disconjunction (O). The last row (R) is the result of the negotiation and the resulting privacy settings for both users.

Table 4.1: User inputs and results

L	A	A	A	O	O	O
P	1	0	0	1	1	0
C	1	1	0	0	1	0
R	1	0	0	1	1	0

The important part to note is that neither user ever gets to see the privacy setting of the other user. For example, if we take a look at Q14 in the previously discussed questionnaire see table3.2. This scenario is a logical conjunction, which means that both users need to agree for it to be enabled. Since neither the patient nor caregiver agrees with this statement, the setting will be disabled. This means that they will be unable to see what the other party answered. While in some scenarios, you would be able to reason what the other party answered based on your input and the result, this overall ensures that no unnecessary information regarding the preferences of either party is given out.
The way the system was made allows us to introduce more complex truth functions in the future. Originally we intended to introduce a third party that would represent the family member of the patient as well, this could easily be done by adding a third Boolean array during the negotiation process. We can also create more complex expressions than just conjunctions or disconjunctions by introducing new arrays that completely overwrite the user's input. An example of this would be the L variable mentioned prior (see table 3.2).

4.3 Integrations

4.3.1 Java

Java Standard Edition was our Java edition of choice. We used version 16.01 when developing our software. Java has several components that are being used to either run or make our software. In this section, we will go into short detail explaining their purpose.

Java Development Kit

Java Development Kit is the tool used to create Java programs. It includes javac, which is used to compile Java code; the java interpreter which converts the java code into machine code; the Java Runtime Environment and several other features necessary for Java Development[8].

Java Runtime Enviroment

The Java Runtime Environment is what allows the user to execute and run Java code on their system. It contains the various default libraries included in Java; the Java class loaders; and the Java Virtual Machine. In our software, JRE is only used on the server. Android has its own set of custom libraries based on JRE instead that replicate most of its functions[9].

Java Virtual Machine

The Java Virtual Machine is the component of Java that handles resource management. It is executed by JRE and is where the Java bytecode is executed. Similar to JDK, Android has its own version of this called Dalvik Virtual Machine. DVM has a focus on optimization which is beneficial for phones with limited memory and processing power[10].

4.3.2 Gradle

Gradle is a build automation tool commonly used for Java projects. It has comparatively high performance compared to many of its competitors, like Maven or Apache Ant and is also fairly lightweight. It is considered the official Build Tool for Android Development and is integrated into Android Studio by default. This made it a natural fit for our chosen build tool when developing the client.

4.3.3 SQLite

SQLite is a Structured Query Language database. It is lightweight, requires no network access, and is open source. It supports embedded relational database features[11]. SQLite requires no installation or drivers to install. It is ACID compliant which ensures reliable database transactions. As the name suggests, SQLite is very lightweight, usually only requiring a couple of megabytes for a small-sized database. The default library is only about 250 kb. By default, SQLite can be managed from the command line, but third-party tools exist that let you manage it from an interface. Overall, the lightweight nature of SQLite combined with its flexibility made it a good choice for our project.

4.3.4 Java Database Connectivity

Java Database Connectivity is an API that allows connectivity between a java program and a database. In the context of our application, it is being used in the server to access the database and perform queries. We also required a specific driver that was compatible with SQLite, as that was our database of choice. Thankfully, an easy-to-use open-source alternative was available to use.

4.4 Database Structure

The following section includes details about the structure of our database. Note that this database was mostly set up for the purpose of being used with our prototype, and may as a result be missing tables or data entries that one might expect to see in other applications (for example, features related to 2-factor authentication, profile pictures or other features that has not been implemented). The UML diagram below shows the current structure of the database.

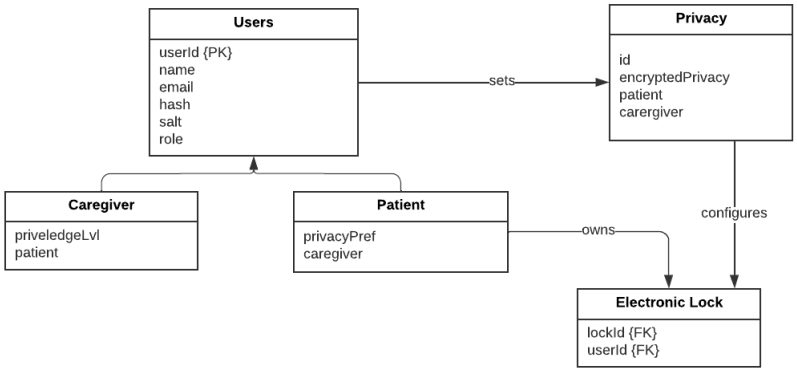


Figure 4.2: UML Diagram

4.4.1 Users Table

The user's table contains information in regards to authentication and user roles. This table is inherited by two additional tables for both Patients and Caregivers. The Patient table, the Patient table has the patient's associated caregiver stored in it. Currently, only one caregiver can be assigned to a patient, but several patients can be assigned to a caregiver. If we were to change this in the future however it could make sense to introduce a separate table that has all patient-caregiver relations stored. The Patient table would likely expand in the future and include several new rows based on what additional data the application might require. The Caregiver table is currently unused but has a column for privilege level. This could potentially be used in the future to allow caregivers to bypass the privacy negotiation if needed.

4.4.2 Privacy Table

This table stores the current privacy settings of the users. The encryptedPrivacy data column is a string of 0's and 1's that each represents the current privacy setting of the user that has been encrypted. When negotiation has happened, and new settings have been enabled, this will be written over again. The caregiver and patient columns are used to determine to whom the privacy settings belong.

4.4.3 Electronic Lock Table

This table would contain the necessary information required to implement the electronic lock. We can't say for certain exactly what would be needed in this table, as we currently don't have access to the API. However, we would likely need some sort of identifier that would allow the software to connect to the right electronic lock and some sort of authentication. We decided to include it to show the relationship between the Privacy Table and integrated devices (e.g locks, cameras, and such).

4.5 Server Environment

4.5.1 Virtual Machine

The server is currently running on a Ubuntu 20.04 LTS virtual machine in the NTNU OpenStack cloud service. It can be reached with the public IP of 10.212.140.133, and the private IP of 192.168.0.194. Originally, we intended to have several virtual machines running on the same network running together, where one would host the database and another would host the software itself. We were also considering the use of Docker for easy deployment. While this would be better than our current system with a single virtual machine, we, unfortunately, had to cut that idea because of time constraints.

4.5.2 Security Groups

Security Groups act as a virtual firewall on the server. By using them we can limit the data that are able to reach it, and therefore decrease the risk of the server being compromised. Currently, we have the following rules enabled by the security groups.

- TCP inbound and outbound on port 22
  Port 22 is commonly used to connect via SSH, which is what we use for managing the server. It also lets us update the server directly from our git repository.
- TCP inbound and outbound on port 3030
  This is the port currently used to both send and receive data from clients.

For updating the virtual machine, we would also require to open port 80 for TCP (HTTP) and port 53 for UDP (DNS). These are currently disabled but can be opened up if necessary.

4.6 Security Features

Since we are Cyber Security students, we've decided it was important to include several security features in our software. While security was not our main priority when developing the software, there were certain aspects we thought were important to consider in regards to security. Here we will go into detail about them.

4.6.1 Input sanitization

An SQL injection is the insertion of malicious SQL code through user inputs. This could potentially compromise our database. To ensure that our database was secure from these sorts of attacks, we implemented input sanitization on all of our database queries. This is achieved by using Prepared Statements. In a normal database query, the data is simply inserted into the database query to form a single statement. This could allow the user to potentially insert malicious code into the query which would be executed on the database, like in the code sample below.

```
String query = “SELECT id FROM User WHERE name =” + userInput;
//User enters “OR 1=1;” as user input
SELECT id FROM User WHERE name = OR 1=1;;
//The query is now sent to the database
//where the malicious code is executed
```

When using Prepared Statements, we instead create a template with the query separated from the user input. These values are then sent to the database as their literal values, instead of as part of a statement.

```
String query = “SELECT id FROM User WHERE name = ?”;
preparedStatement.setString(1, "userInput");
//User enters “OR 1=1;” as user input
//Since the query is separated from the user input,
// it will not be ran as malicious code and instead
//inserted into the database as it’s literal value
```

4.6.2 Password Hashing

All passwords being stored in the database are hashed before they are saved. This process ensures that if the database were to be compromised, no passwords would be able to be gained from it. As recommended by the Norwegian Data

Protection Authority, we are using the OWASP Password Storage Cheat Sheet as a basis for which algorithm to use. Out of the options there, we chose Argon2id as it is considered a modern and powerful hashing algorithm that is more than sufficient enough for the scope of our project.

4.7 Yao's Garbled Circuits

There were several options when determining which form of negotiation to use. Originally, we intended to use Yao's Garbled Circuit cryptography protocol for the purposes of negotiation, but this was unfortunately scrapped because of time constraints. Note that as mentioned prior, this project is intended to be a proof of concept and that therefore this doesn't change the end result. Our current software is made with the intent of being able to implement Yao's Garbled Circuit in the future, with some minor changes. Despite not being able to implement it properly into our project, we still thought it would be important to have a section detailing why we believe the Garbled Circuit would be advantageous for our project.

4.7.1 Background

The Garbled Circuit cryptography protocol was introduced by Andrew Yao in 1986[12] in the oral presentation of the paper "How to generate and exchange secrets"[13]. It is a safe way for two parties to jointly compute a function with their private inputs[12]. This is what mainly differentiates it from our current system. Currently, we require three parties, the patient, the caregiver, and the server, to complete the negotiation. With Yao's Garbled Circuit we could instead cut the server from the negotiation process (it would still help connect the different users, and to authenticate and manage the electronic locks). This would be done through a peer-to-peer system in combination with our client-server model.

Garbled Circuits allow two parties, having inputs x and y, respectively, to evaluate an arbitrary function f(x,y) without knowing the other party's inputs beyond the output generated by the function[12]. Party A, called the GC generator, creates an encoded version of a circuit that computes f, while party B, called the GC evaluator, computes the output of the circuit without knowing the other party's information. The protocol is safe as long as both parties follow it as intended.

$$(y_1, y_2) = f(x_1, x_2) \tag{4.1}$$

Party 1 has x_1 and wants to know y_1 Party 2 has x_2 and wants to know y_2. But party 1 does not want party 2 to learn x_1 and vice versa. It is important to first describe the mechanism to build the circuit required for the protocol. Let us consider the simplest version, logical disjunction (OR) with the garbled circuit. Here, our goal is to encrypt every gate. We

will express the function as encrypting each gate because that is what the Garbled circuit does. According to this concept, each wire w_i within the circuit can have two values, 0 or 1. and we can associate those values 0, or 1 to two symmetric keys. If we then assign two (symmetric) keys k_i^0 which corresponds to 0 values and k_i^1 which corresponds to 1 value to each wire, each wire can have one value. Every gate G is represented by a function with two input wires and one output wire.

In the following example (see table 4.2), we have an encryption table. After we garble said table, we get resulting (see table 4.3) output. Again, if this message is encrypted with association keys to w_i and w_j, by assuming a symmetric two-key encryption function Ek,k'(m) IND-CCA (indistinguishability under adaptive chosen-ciphertext attacks), see the table 4.4. The next table shows a garbled gate, where each gate in the circuit has four ciphertexts (table 4.5).

Table 4.2: AND Gate Encryption

w_i	w_j	w_k
0	0	0
0	1	0
1	0	0
1	1	1

Table 4.3: Garbled or Encrypted

w_i	w_j	w_k	m
0	0	0	k_k^0
0	1	0	k_k^0
1	0	0	k_k^0
1	1	1	K_k^1

Table 4.4: Symmetric encryption

w_i	w_j	w_k	c
0	0	0	$k_i^0\ k_j^0(k_k^0)$
0	1	0	$k_i^0\ k_j^1(k_k^0)$
1	0	0	$k_i^1\ k_j^0(k_k^0)$
1	1	1	$k_i^1\ k_j^1(k_k^1)$

Table 4.5: Garbled gate, so that each gate in the circuit has four cipher texts

c
$k_i^0\ k_j^0(k_k^0)$
$k_i^0\ k_j^1(k_k^0)$
$k_i^1\ k_j^0(k_k^0)$
$k_i^1\ k_j^1(k_k^1)$

Table 4.6: Gate Evaluation, decrypting the second row

c
$E_k i^1, k_j^1(k1k)$
$E_k i^0, k_j^1(k_k^0)$
$E_k i^0\ , k_j^0(k_0^k)$
$E_k i^1, k_j^0(k_0^k)$

Gate Evaluation

When evaluating the gate, assume the user learns the value of the wire label for the 0 value on wire i and the 1 value on wire j. He learns k_i^0 and k_j^1. Note that he does not know that wire i is 0 and wire j is 1. With these values, they can decode only one row of the table. If they were to try all the rows, only one row would actually be decrypted (see **??**). Therefore we need an IND-CCA scheme because it rejects invalid ciphertexts. We can only decrypt the second row. Hence we learn k_0^k and k_k^0, but we have no idea it corresponds to the zero value on the output wire (table **??**).

Chapter 5

Development Process

5.1 Justification

To justify the need for our project, we have separated this section into the following parts: Motivation (what prompted us to conduct this study), importance (what is the relevance of this study to the state of knowledge), and utility (how will the results be used to solve the problem).

MOTIVATION: The motivation for this study lies in the urgent need to protect the privacy of individuals while they are under surveillance. This is because some of the privacy-enhancing technologies that have been introduced into monitoring systems in the patient environment raise ethical issues. Therefore, a software agent is needed to synchronize communications between patients and caregivers in a private environment in a secure manner.

IMPORTANCE: Currently, much research is being done to protect patient privacy. But it is still difficult to find out a person's privacy attitudes and behaviors when being monitored because patients have different privacy attitudes and preferences. Therefore, the results of this study will provide valuable reference information to the NTNU e-HWS research group. For example, the survey conducted will serve as input for the software application developed to negotiate privacy settings between caregivers and patients. In addition, these studies will serve as the basis for related research on privacy in the elderly.

UTILITY;- The results of this study will provide a critical assessment of current privacy concerns in improving technology for monitoring elderly or patients in terms of long-term privacy protection, and provide an opportunity to continuously improve patient privacy settings by developing the presented software agents based on technologies such as logical computation like AND / OR, or if implemented, the Garbled circuit and Oblivious transfer would be appropriate tools to establish trust between two parties. in the process of negotiation in application development.

5.2 Execution

The project work officially on January 11th, 2022 after an orientation. We started working on the project plan in January, and at the same time spent two weeks reading topic-related documents and gathering information to understand user requirements and identify the design model. Finally, we decided to proceed with the Android application. Both the application development and the dissertation work started after we submitted the project plan on January 31. The development of the application began in early February. First, we created a UI prototype that would reflect the look and feel of the client. Basically, the goal of a prototype is to test and validate ideas before sharing them with stakeholders and eventually releasing the final designs for the development process. Click on this link to see the UI prototype.

5.3 Choice of programming language

Deciding which software language to use was an important decision to make early on in the project lifespan. Since we decided to make an android application it was important that it was well suited for android development.

5.3.1 Kotlin

Kotlin is the "official" language of Android development. It is considered very easy to learn and very powerful, combining both object-oriented and functional programming While Kotlin was first released in 2011, it wasn't until recent years that it gained a lot of popularity. This means that it is somewhat lacking in publicly available APIs compared to other languages. Kotlin is also mostly used for the purposes of Android development, while other options would allow us to focus on using a more flexible language that could serve us in future job prospects.

5.3.2 Java

Java is one of the most common languages for Android development. It is considered very flexible and is often used for various kinds of projects outside of Android developments, like desktop apps or servers. Because of its popularity, there was a lot of documentation available that we could use to research the best practices when developing our application. One of the downsides with Java, compared to Kotlin, is that it is somewhat less concise. This means that writing code will often take a long time which could be a serious risk considering our time restraint.

5.3.3 Other

While Android applications are usually made with either Java or Kotlin, other alternatives exist too. The Android Native Development Kit allows for applications made with both C and C++, this is less flexible than Java or Kotlin however and has other challenges associated with it, like less support and difficulties setting up.

5.3.4 Conclusion

In the end, we decided to go for either Java or Kotlin. Both had their advantages and disadvantages. The deciding factor was Java's popularity, even outside of Android development. This meant we could apply what we learned easier to future projects. Another deciding factor was the available documentation for Java, which exceeded that of Kotlin, making it easier to research.

5.4 IDE

We used several IDEs during the development of our application. During this section, we will briefly discuss them and how we used them.

5.4.1 Android Studio

Android Studio was our IDE of choice when developing the client. It is developed by JetBrains and Google and is intended for being used in Android projects. It includes many convenient features, like being able to create a UI through a graphic interface, Android-specific code refactoring, and a built-in Android emulator for testing purposes. It is based on IntelliJ IDEA.

5.4.2 IntelliJ IDEA

IntelliJ IDEA is an IDEA developen by JetBrains. This was our primary IDE of choice when developing the server. It shares many similarities to Android Studio but is centered around non-android Java development. While it would be possible to develop the server through Android Studio, we found it easier to use IntelliJ IDEA for the server because of the cleaner interface without the Android unnecessary Android features.

Chapter 6

Deployment

6.1 Deployment

The client is deployed in an Android application PacKage (APK) and can be manually installed on the user's devices that are running Android 11 or higher. Most Android devices require you to enable the installation of APK files from unknown sources for security reasons, on the majority of devices this can be done by going into the device settings and enabling the "Install unknown apps" permission. Alternatively, the application could be published on Google Play Store, in which case you would not be required to enable the permission for installations.

The server is currently deployed on a Ubuntu 18.04 LTS virtual machine running on the NTNU Openstack environment, however, it can be deployed in any cloud environment that is capable of running SQLite, and Java SE. The server also needs to allow TCP in and out on port 3030 to be able to communicate with the client. The project is currently stored in our BitBucket repository[14], and also on the NTNU's own GitLab enviroment[15].

6.2 Testing Methodology

In this section, we describe software application testing and take a look at the definition of software testing and the explanation of the corresponding types of software testing. Basically, software testing is an investigation that is performed to provide partners or stakeholders with information about the quality of the products. Software testing can also provide an objective, independent view of the software to allow the business to appreciate and understand the risks of software implementation [16]. According to Dave Gelperin and William C. Hetzel[17] Software testing can be stated as a process of validation and verifying and validating that a software product meets its requirements that guided its design and development, works as expected, can be implemented with the same characteristics, and satisfies needs of stakeholders. The purpose of testing is to

discover software defects so that the defects can be corrected. Testing can be used to determine when a product will work properly under certain conditions. Testing involves examining code and executing that code to verify that the code does what it is supposed to do. In our case, we used an Android emulator to test our code in sequence. Basically, an Android emulator simulates Android devices on our computer so that we can test our homecare application on a variety of devices and Android API levels without having to own each physical device. One of the advantages of testing applications on an emulator is that it is easier and faster than testing on a physical device. To this end, we installed the Android Emulator and selected the appropriate Android Emulator component from the SDK Tools tab of the SDK Manager. To effectively test the application, we created an AVD (android virtual device) that models the devices we want to run our application on, e.g. $pixel3XLAPI30$, $pixel_3a_API_30_x86, ...etc$.

6.3 Quality Assurance

In this section, we will describe in more detail whether the system meets the project requirements. The design part of the Android application is most likely fulfilled. For example, the system responds to the registration of new user roles as well as to the authorization of the login of system users. The negotiation part, which is the backbone of the whole application and part of the main project requirement, has been applied in the design parts. The functions of this software agent are as follows: The application allows users to synchronize their privacy settings, for example, the system synchronizes the privacy settings of patients and medical staff (whether to monitor the patient or allow visitors to access the code of the electronic lock, etc.).

6.4 Scalability

The software was designed with scalability in mind. It is very easy to implement new features by creating new states in the finite state machine on both the server and the client. Since most of the logic takes place on the server, this means that the new functions do not necessarily affect the performance of the client. The server can be scaled both horizontally, by introducing a load balancer, and vertically, by improving the specifications of the virtual machine on which it runs.

Chapter 7

Discussion

This research and the development of the project aimed to investigate the research question and develop a mechanism to improve patient privacy in nursing homes using an Android application designed to negotiate conflicts in the scheduling of assistance to patients by nursing staff.

7.1 Discussion regarding the final product

After understanding the project description, we first looked for a research question. We came up with unstructured research questions, meaning we expanded the scope of the scenarios and included many questions. After a while, we had a weekly meeting with our partners where we learned that it was not possible to expand the scope due to time constraints. So we decided to shrink or narrow the scope and focus on certain scenarios, so we turned our unstructured research questions into structured research questions.

To find out about patients' privacy and behavior when they are being monitored or are scheduled to be helped by caregivers, it is very important to consider patients' privacy concerns. We guess that we will develop a software agent that securely synchronizes communication between multiple parties and establishes an agreement.

As a first step, we decided to conduct data collection using a real-life scenario in a nursing home. This involved the user roles that are directly related to each other in nursing homes, such as patients, caregivers, and patient's families. For this purpose, we compiled 15 questions for two user roles and 10 questions for one user role on the scenarios of electronic door locks, camera and other surveillance technology, and other incidents. Accordingly, the respondents answered the distributed questionnaire. After the collection was completed, we analyzed the response feedback based on logical computation AND/OR. Then we identified where conflicts in feedback between user roles occurred.

7.2 Our methodologies

Collecting information about individual privacy preferences is an ongoing process. You do not do it once and then forget about it; you do it every time because everyone's privacy preferences are different or vary from person to person. In exploring software-based negotiation of privacy settings with introduced home care monitoring technologies to protect patient privacy, our two methodologies mentioned above in Section 2.1 of Chapter 2 proved useful.

To answer the research question, we developed several questionnaires to be answered by three user roles (patient, caregiver, and family members of patients). A plan of how data collection could be conducted is detailed in Chapter 2(see subsection 2.2.2).

In the time we have been writing this paper we have learned a lot, but there are still things we would have liked to have done differently and separately for each group if we had enough time, which is listed below.

The context of enhancing privacy for the elderly living in a home care environment is very broad. If someone is concerned with the care of the elderly, the focus should be clearly defined, because the elderly are divided into different categories depending on their health status. The elderly are either placed in a facility called a care center or at home. Those who are placed in a care center are mostly elderly people who have dementia, Parkinson's, Alzheimer's..etc. This category includes elderly people who cannot manage their daily activities independently and others who belong to a different age group but cannot manage their daily activities independently due to certain disabilities. The same scenario is not designed for each group, and the application design should also be tailored to each group. For example, the application designed for elderly people with dementia with scenarios such as an electronic door lock and camera cannot be used for other elderly people without dementia.

Data collection, which is the main input for the development of the application, should be done separately for each group. On the other hand, older people who live in their own homes but receive care in a nursing home have different aspects of privacy than those who live in a nursing home. Data collection for this group should also be used to design the application for this specific group.

7.3 Learning outcomes

During the project period, we've learned many valuable things within our field of study. In this section, we will discuss some of them in detail. First and most it is our first time working with such a big project which has both research and development parts. We learned how to formulate a research question about our dissertation topic. Based on this, we developed a questionnaire to collect real-life data, and based on the feedback, we developed a responsive application to help negotiate conflicts between multiple parties.

Another valuable asset we gained from our project was the understanding of Android development, which was new to both of us. Understanding the unique Android-specific syntax and best practices took a while but was very valuable in the end. There are many other parts of Android development that we haven't touched on during our project, like compatibility between different types of devices (e.g. Android TVs, or Chrome OS devices) or different language support. What we have focused on however has been very informative.

We can't ignore the security aspects that we've had to focus on either, like learning how to protect against SQL injection or using client-server architecture to separate responsibility between the different parts of the system. These are of course just a couple of examples of what we've learned throughout the project and overall, the project has been very educative for both of us.

Chapter 8

Conclusion and Future Works

8.1 Conclusion

We believe that our software agent works are a good solution to the issues presented in this thesis. By automatically negotiating the privacy settings between the caregivers and patients, we remove a lot of potential stress and time that they would otherwise have to spend on it. We can also control it in our own environment where we can take measures to decrease the risks associated with storing privacy settings.

We have created the appropriate questions under all the scenarios we need for our expectations and distributed the questionnaire. We received feedback from all three intended user roles (caregivers, patients, and families/relatives). But when collecting data, it was not easy to contact those directly affected. It was a great challenge to contact the management of several nursing homes by email and phone, but unfortunately, we did not receive any response except from one nursing home. We successfully conducted one user role from preferred home care and for the remaining two user roles we used Plan B, only families, and friends who have a health background and work in health care.

Proper data collection is very important because it is the most important input for the development of the application. This data collection should be done separately for each category of the elderly. Depending on the category, older people have different sensitivities about privacy. For example, older people who have dementia and live in nursing homes have very different privacy concerns than those who receive home care at their homes. Therefore, proper data collection is very important for setting the privacy of individuals in the proposed application.

So far, we have discussed technologies such as Yaos Garbled Circuit or Oblivious Circuit and Logical computation conjunction(AND) and disjunction(OR) in our development as a negotiation template for the preferred privacy option among multiple options in a question for specific user roles in a scenario such as electronic door lock, camera surveillance, and other incident scenarios, as we have already discussed in Chapter 3, **??** and Chapter 4, 4.2.

In addition, we used SQLite to store the data on the user's device in the form of a text file. This is an open-source database that is built into Android. We created a backend-like server to provide the trust with the third parties and compare the results. For security reasons, we placed it on the NTNU SKYHIGH cloud platform.

8.2 Future Work

8.2.1 Electronic Door Lock

The system we have created allows for the integration of various electronic devices, out of these we put the most focus on an electronic lock. It would lock and unlock based on the negotiated privacy settings configured in the application. Unfortunately, we were unable to acquire access to the door lock API in time. While it's difficult to say exactly what we would require to implement the Door Lock, the software was made with the purpose of being able to manage it, so it would likely be fairly easy to implement.

8.2.2 More Comprehensive Study

If given the time and resources, we think it would be optimal to perform the study previously discussed in this thesis on a larger target group. Currently, the sample size was very small, which means that the results gained from the study are not as conclusive as we'd like. While this serves the purpose of developing our proof-of-concept, it would be preferable to perform the study with a larger group.

8.2.3 Scalability

The server is currently running on a very minimalist setup that wouldn't be able to handle an influx of users. While the current setup works well in our limited environment, there would have to be changes made to accommodate more users. The best starting point for this would be via vertical scaling by increasing the computing power of the server. Alternatively, we could introduce horizontal scaling via load balancing or Infrastructure as Code methods.

8.2.4 UI improvements

Most of the user interface currently uses default Android UI Controls with some changes to the XML. This could be improved upon to create a better user experience with custom-made controls that better suit our project.

Appendix A

Additional Material

The following appendixes contain the result of our study. The caregiver survey study was performed by actual caregivers wom are working in selected care-center and willing to participate in data collection, while the patient and parent survey study was performed by friends and families whom have working in health care and willing to put themselves in the position of either patients or families. These results were then separated into the statements mentioned in section 3.2. This study was meant to serve as an example of what an larger study might look like, to help gain insight into which scenarios makes sense to implement.

The study was performed on nettskjema.no and is completely anonymous. Before being allowed to and all participants had to sign a consent form detailing what we would use their data for, and how long we would store it. Note that although the consent form did not mentions any thing about personal information.

We have also included our project plan, to provide insight into how our initial plans have changed from the beginning of the project. At the very bottom we have included the prototypes.

Rapport fra «Homecare questionnarie for Caregivers»

Innhentede svar pr. 9. mai 2022 21:18

- Leverte svar: **3**
- Påbegynte svar: **0**
- Antall invitasjoner sendt: **0**

Med fritekstsvar

Q1) When you are visiting a patient who is staying in his/her care home and he/she is in good health. Which of the following measures is better suited for the situation? *

Svar	Antall	Prosent
I would like the patient to open the door for me, since he/she is in a good condition. I will respect their privacy.	3	100 %
I would like to get access to their room via the electronic door lock directly because I've made an appointment with them directly. And they should be notified about my arrival in advance.	0	0 %

Q2) When the patient is visited by their parents in normal health condition, who do you think should open the door for the parents? *

Svar	Antall	Prosent
I think the electronic door lock should open the door automaticaly since the parent has been given permission and recording tecknologies or cameras are deactivated automaticaly if present in the patients room.	1	33,3 %
I think the parents should inform the caregivers first, then caregivers are resposible for unlocking the door for parents since they have access permission.	0	0 %
I think the patients should open the door for their parents themselves when they for visit.	2	66,7 %

Q3) When physiotherapists come to visit patients at their care home. Which of the following do you prefer?

Svar	Antall	Prosent
The physiotherapist should open the door themself, as long as I've given their consent beforehand.	0	0 %
I would like if the physiotherapist would contact me first so that I can open the door.	2	66,7 %
I would like the caregivers to facilitate the visit and make sure the patients privacy is being protected.	1	33,3 %

Q4) When you visit the patient while they're busy doing other things and they don't want to be disturbed, what should be appropriate for the situation?

Svar	Antall	Prosent
I would prefer if the patient themself opened the door once they are finished with whatever they're doing. After proper communication (via video chat) has been done. The patient have the right to say no.	2	66,7 %
I prefer to open the door myself, since I have been given access and concent.	0	0 %
I prefer to open the door myself to ensure they're not in a life threatening situation.	1	33,3 %

Q5) When you come to visit the patient and he/she is unable to open the door. What would you prefer to do in this kind of scenario?

Svar	Antall	Prosent
I would like to talk to patients via video call or send a recorded message to ensure the patient is safe.	1	33,3 %
I would like to open the door first and talk to users later, since I have been given permission.	2	66,7 %

Q6) When you come to visit a patient and he/she is not willing to open the door or giving consent, what is appropriate for this situation?

Svar	Antall	Prosent
I would like to follow up the patient by whatever means of communication that is available to find out what is wrong with them.	1	33,3 %
I have no rights to open the door unless the patient would be found to be in danger, in this case I'm obliged to open the door since I have access permission.	2	66,7 %

Q7) While you are visiting a patient who is not willing to open the door and not giving consent, but have relatives around, what is appropriate in this situation?

Svar	Antall	Prosent
I would prefer for the patient to decide in this type of situation, since they have right to refuse opening the door. If they refuses to let us in, we need to respect their choice.	2	66,7 %
I would like if the parent could come and open the door for us, to ensure the patients safety.	1	33,3 %

Q8) When you come to visit a patient with a serious condition and he/she is unresponsive, what is appropriate in this situation?

Svar	Antall	Prosent
I would open the door myself and offer the necessay care and assistance for the patient, since I have access permission.	2	66,7 %
I would prefer if the patient open the door for me if they're capable, since I want to respect their privacy.	0	0 %
I would like if the eDoor_lock unlocked automatically in cases of emergency, if it detects that the patient is in unconscious condition.	1	33,3 %

Q9) Assume the patient has some form of alarm that detects incidents (e.g a fall alarm). While the patient is taking a shower or getting dressed, and is suddenly exposed for a serious medical condition (e.g. heart attack or a seizure), what is appropriate in this situation?

Svar	Antall	Prosent
I would prefer if the alarm is triggered automatically and notify me immediately in case of incident.	2	66,7 %
I would prefer if the patient themselves manually had to hit the alarm button when they realize there's symptoms.	0	0 %
I prefer if there was a system in place that could automatically take care of the patient based on their predefined privacy settings.	1	33,3 %

Q10) When the fire alarm goes off while the patient is in his/her care home, who do you think should open the door?

Svar	Antall	Prosent
I would like the eDoor_lock to open automatically once it detects the fire alarm , since saving the patients life should be prioritized first.	3	100 %
I would prefer to open the door myself, since I have access right and to ensure the personal privacy of the patient is kept intact.	0	0 %
I would like as firefighters to open the door and evacute patients.	0	0 %
I would like the patients to open the door by themselves.	0	0 %

Q11) Police is visiting after receiving a call from a patient, what is appropriate in this situation?

Svar	Antall	Prosent
I would like if the patient themselves can talk to the police and discuss their problems without caregiver interferance.	3	100 %
I would like if the police contacts the nursing home centre's manager directly to resolve the issue.	1	33,3 %
As a caregiver, I will not let anyone in without a good reason. So the police must have good reason to enter.	0	0 %

Q12) While the patient is in his/her room doing activities like making their bed or cleaning and suddenly exposed for a fall accidents, what is appropriate in this situation??

Svar	Antall	Prosent
I would like if some sort of monitoring technology like a camera would be activated in the patients room and signal that they may need assistance.	1	33,3 %
I would like if there was a system in place that allows patients themselves to notify emloyees of the centre about the incident.	2	66,7 %
I would prefer if the patients environment could be controlled automatically by smart appliances to do their activities (e.g. dishwasher, Roomba) to minimize risk.	0	0 %

Q13) If the patient is found to be suffering from a chronic disease like diabetes, dementia or facial weakness, what measures do you think should be taken?

Svar	Antall	Prosent
I would like if tools like cameras or other fall assessment tool were installed to assist the patient.	1	33,3 %
I would like if we made regular follow ups and provided further assistence to the patient to fulfill their needs.	2	66,7 %

14) How does the patients overcome the feeling of isolation? Is there any mechanisms you prefer to help the patient with these issues?

Svar	Antall	Prosent
I would like if communication devices would be installed in patient room to reduce the feeling of isolation.	1	33,3 %
I would like if the patient exposed for feelings of isolation would participate in local social engagement activites.	2	66,7 %

Q15) How does the patient control irregularities in sleep and meals? Is there any control mechanisms or devices in place to help them?

Svar	Antall	Prosent
I would prefer if a sleep, eating, or exercise alarm could be installed in the patients room.	2	66,7 %
I would prefer if technologies like appliance assessment of abnormal sleeping patterns could be installed in the patients room.	0	0 %
I don't think devices like that would be neccessary. Patients can manage it themselves with the help of a caregiver.	1	33,3 %

Q16) What do you prefer to control the patients virtual social activities like gaming, online relationships, chatting with friends, etc.?

Svar	Antall	Prosent
I would like if the patients personal information could be written down physically in case they forget their login information.	1	33,3 %
I would like it if the patients personal information could be encrypted and only accessable by them to protect their privacy.	3	100 %

Rapport fra «Homecare questionnarie for Patient»

Innhentede svar pr. 10. mai 2022 11:48

- Leverte svar: **3**
- Påbegynte svar: **0**
- Antall invitasjoner sendt: **0**

Med fritekstsvar

Q1)When you are going to be visited by caregivers while you are staying at your care home and you are in good health condition. You have made the appointment with your caregiver in advance. Which of the following ways do you prefer in this situation? *

Svar	Antall	Prosent
I would like myself to open the door for caregiver. Since I am in good condition, I do not need the electronic door lock to directly open the door for caregiver to help me immediately. If care providers comes in directly, it will intrude my privacy.	1	33,3 %
I would like as caregiver get access to my room once she/he arrives, because we will have an appointment and I will be notified about her/his visit in advance.	2	66,7 %

Q2) When you will be visited by your parents at your care home while you are in good health condition. Which of the following way do you prefer best? *

Svar	Antall	Prosent
I would like to open the door by myself since I am in good health condition and i am not allowed as electronic door lock unlock automatically. If not it is a breach of confidence.	2	66,7 %
I would like as caregiver get access to my room once my parent comes for visit, because we already have an appointment and I will be notified about my parents visit in advance.	1	33,3 %

Q3) When physiotherapy comes to visit you at your care home which measure do you prefer best? *

Svar	Antall	Prosent
I would like myself to open the door for physiotherapy who comes to visit me.	1	33,3 %
I prefer as caregivers will facilitate and make sure I am informed in advance.	2	66,7 %

Q4) When caregivers come to visit you at your care home, while you are busy doing other things and you do not allow to get disturbed. In this situation what do you prefer best? *

Svar	Antall	Prosent
I would like myself to open the door for caregiver when I finish my work. Since I don't want to get disturbed, I do not need the electronic door lock to unlock directly. If caregivers comes in directly, it will intrude my privacy.	1	33,3 %
I would like caregivers to get access to my room later once I finish my job. Before that I will not allow anyone to disturb me.	2	66,7 %

Q5) When caregivers come for visit and you are unable to open the door. What would you prefer best in such scenarios? *

Svar	Antall	Prosent
I would like as caregivers can talk to me via video call or sending recoded message to know my state.	2	66,7 %
I would like as caregivers to try to open the door first and talk to me later.	1	33,3 %

Q6) While you are not willing to open the door as well as not giving consent to caregivers, in such cases what would you prefer to happen? *

Svar	Antall	Prosent
I would like as caregivers must follow my state using available means of communication to know what is wrong with me..	0	0 %
As long as I have right to say no, no one would be permitted to open my door, unless iam in danger. But in severe case caregivers can open the door.	3	100 %

Q7) While caregivers come for visit and you are not willing to open the door as well as not give consent, but relatives are around with you, whom do you think will open the door? *

Svar	Antall	Prosent

Svar	Antall	Prosent
I decide myself because I am the only one who have right to open the door, at this moment since I do not want any help from caregiver I prefer to stay alone with my family members..	3	100 %
I would like as my family members can decide whether caregivers would come in or not.	0	0 %
In this case I would like as my family members can open the door and set the necessary privacy preferences (e.g., whether to be recorded during the visit) for me.	0	0 %

Q8) When caregivers come to visit you for emergency condition and you are in unconscious condition. In such cases who would you like to open the door to offer you necessary assistance? *

Svar	Antall	Prosent
In this case I would like as caregivers will open the door and offer me the necessary care and assistance since I am in need of help.	3	100 %
I prefer in this scenario my family members will open the door if they are available around.	0	0 %
I prefer myself to open the door since I care about my privacy. Only if it's extremely severe will I allow caregivers to open the door.	0	0 %

Q9) While you are taking a shower or getting dressed, suddenly exposed for heart attack, or having a seizure. What would you prefer best? *

Svar	Antall	Prosent
I prefer as alarm can be set to the on mode automatically and caregivers will open the door after they get signal on the spot with integrated technology.	1	33,3 %
I prefer myself to hit alarm button immediately when I realize the symptom.	2	66,7 %
I prefer there can be a system in place that could automatically take care of me based on my predefined privacy settings.	0	0 %

Q10) While you are at care home and if fire incidents happen whom do you think open the door? *

Svar	Antall	Prosent
I prefer as electronic door lock will open the door automatically once fire alarm break out happens, since I prioritize my privacy i would not allow anyone to come into my room.	2	66,7 %
I wish as caregiver will facilitate the process for me since I prioritize life saving first.	1	33,3 %
I would like as firefighters will open the door and rescue me.	0	0 %
I would like as myself will open the door to escape from a fire.	0	0 %

Q11) When Police come to visit you after receiving a redundant call from you. which ways do you prefer in such situation? *

Svar	Antall	Prosent
I would like as myself contact the police and discuss my problem without caregivers interference.	2	66,7 %
The police must have a good reason to enter. Caregivers should not let anyone in without this being clarified.	1	33,3 %
I would like if the police contacts care home centre's manager directly to resolve my issue.	0	0 %

Q12) While you are in your room doing home activities like making bed and putting things in place, suddenly exposed for fall accidents. What do you prefer if such cases happen? *

Svar	Antall	Prosent
I would like as monitoring technologies like camera would be activated and send automatically anonymous pictures or signal alarm for caregivers to get necessary assistance.	2	66,7 %
I would like as myself would hit alarm button to notify the caregivers of the centre.	1	33,3 %
I would like as my environment could be controlled automatically by smart home technologies (e.g., heat, electricity, washing machine, and light).	0	0 %

Q13) While you are suffering from chronic disease like diabetes, dementia, facial weakness detected and others, How would you like to be monitored?

Svar	Antall	Prosent
I would like to have regular caregivers follow up and assistance I need.	1	33,3 %
I would like as assisting technologies like camera and other recognition appliances could be installed and assist me.	2	66,7 %

Q14) How do you overcome the feeling of isolation? Is there any mechanism you prefer to help you in this

condition? *

Svar	Antall	Prosent
I would like as communicating devices(e.g, voice friends devices) would be installed in my room and help me to reduce my feeling of isolation.	1	**33,3 %**
I would like as caregivers will assist me to participate in social engagement activity once I develop isolation feeling.	3	**100 %**

Q15) Do you have strong social connection? if yes, How do you control your virtual social activity like gaming, relationship, chatting with friends, …etc? *

Svar	Antall	Prosent
I would like as I encrypt all my personal information and only accessible by myself to protect my privacy.	3	**100 %**
I would like to store/write all my personal information in book and in case if I forget password to login.	0	**0 %**
I would like as caregivers will help me if i forget to login/logout or help me changing Password every three months.	0	**0 %**

Se nylige endringer i Nettskjema

Rapport fra «Homecare questionnarie for Parent v-ok»

Innhentede svar pr. 14. mai 2022 22:10

- Leverte svar: **2**
- Påbegynte svar: **0**
- Antall invitasjoner sendt: **0**

Med fritekstsvar

Q1) When you visit a patient in his nursing home while he is in good health. Which of the following do you prefer best? *

Svar	Antall	Prosent
I want patient to open the door for me because the patient is in good health	1	50 %
I would like the caregiver to unlock the door for me.	1	50 %
I would like the caregiver to give me permission to open the door myself when I come to visit, since we already have an appointment and I have been informed in advance of my visit.	0	0 %

Q2)Suppose you visit the patient in his nursing home while the patient is ill or in poor health. Who do you think is best suited to open the door? *

Svar	Antall	Prosent
I would like as to be able to unlock the door myself.	1	50 %
I prefer as caregiver should unlock the door for me.	1	50 %

Q3) What would you do if a caregiver comes to visit while you are at home with the patient and the patient is unwilling to open the door and refuses to give the caregiver consent? *

Svar	Antall	Prosent
I prefer to negotiate with the patient first if he/she gives consent or allows me to open the door for the caregiver if necessary	1	50 %
I would like the electronic door lock to automatically unlock once privacy settings have been made	2	100 %
I want to track the patient's condition and have smooth communication to know what is going on with him/her to ensure his/her safety.	0	0 %
As long as the patient has the right to say no, no one should open the door unless she/he is in danger.	0	0 %

Q4) If a nurse comes to visit and the patient is unwilling to open the door, but you are with the patient in his nursing home, who do you think will open the door? *

Svar	Antall	Prosent
I prefer the patient to decide for himself, because he is the only one who has the right to open the door. Since the patient is not interested in letting the nurse in, the patients decision should be respected.	1	50 %
I prefer that I can decide for myself whether a caregiver comes in or not.	1	50 %
I would like to be able to open the door after consulting with the patient to ensure the patient's safety.	1	50 %

Q5) If you visit a patient at home and they suddenly have a heart attack or seizure while showering or getting dressed. What would you most like to do? *

Svar	Antall	Prosent
I prefer the alarm to be set to power on mode and automatically send a signal to the caregiver on site with integrated technology.	1	50 %
I want the system to record the anonymous video as soon as such abnormal activity is detected.	1	50 %
I want the system to record the audio as soon as abnormal activity is detected.	0	0 %
I want the system to monitor me or record any activity whether I am in the patient room or not.	0	0 %

Q6) If you are visiting a patient in a nursing home and suddenly the fire alarm goes off, who do you think opens the door when such an incident occurs? *

Svar	Antall	Prosent

Svar	Antall	Prosent
I prefer as eDoor-lock will opens the door automatically once fire alarm goes off, since i prioritize patient life saving.	2	100 %
I wish as caregiver will facilitate the process for patient since i prioritize patient privacy first.	0	0 %
I would like as firefighters will open the door and evacute patient.	0	0 %
I would like as myself will open the door to escape patient from a fire if i'am at care home.	0	0 %

Q7) If you are visiting a patient and he/she is in the process of putting some things in place, and the patient is suddenly in danger of falling. What do you prefer to do when such falls happen in your presence? *

Svar	Antall	Prosent
I would like to see monitoring technology such as the camera that can be activated and automatically send anonymous images or set off an alarm for caregivers to get the help they need	2	100 %
I want me to press the alarm button to notify the centre's nursing staff	0	0 %
I want the patient's environment (heating, electricity, gas, washing machine and light) to be automatically controlled by smart devices.	1	50 %

Q8) When you visit a patient in the nursing home who has chronic diseases such as diabetes, dementia, facial weakness and others, how would you like to be monitored? *

Svar	Antall	Prosent
I want the system to monitor and record activities because the patient is not in a normal state of health	1	50 %
I would like assistive technologies such as a camera and other fall detection devices to be installed and help the patient.	2	100 %
I want manual caregivers to attend to the patient on a regular basis and help them when they need it	0	0 %

9) If you visit the patient in the nursing home and the patient is in good health, do you want the existing monitoring system in the patient's room to record you talking to the patient? *

Svar	Antall	Prosent
I want the existing system to monitor but not record normal activities.	0	0 %
I want the system to be able to monitor and record activities as before.	0	0 %
I do not want the system to monitor or record activities while I am in his/her care home.	2	100 %

10) If you invite a patient to your home and the patient is in a normal state of health. How would you like the monitoring system to record when abnormal activity occurs. *

Svar	Antall	Prosent
I want the system to record anonymously or record the privacy-friendly video as soon as any abnormal activity is detected.	1	50 %
I do not want the system to record all activity that takes place in my house	0	0 %
I want the system to record audio or send an alarm as soon as abnormal activity is detected.	0	0 %
I want the system to record the sound or send an alarm signal to caregivers.	1	50 %

Se nylige endringer i Nettskjema

Samtykke skjema

☐ Jeg har lest og forstått informasjonen om "Datasamling om Privacy in Homecare" og har blitt tilbud muligheten til å stille spørsmål. Jeg gir samtykke til:

☐ Jeg bekrefter at jeg vil delta i denne spørreundersøkelsen, muntlig eller via tekst.

☐ Jeg bekrefter at jeg har blitt informert og forstår undersøkelsens hensikt, databehandlingsmetode, og mine rettigheter fra informasjons brevet. Jeg har fått tid og mulighet til å spørre spørsmål om spørreundersøkelsen. Jeg er fornøyd med orientering mot spørreundersøkelsen.

☐ Jeg forstår at deltagelsen i spørreundersøkelsen er frivillig og at jeg har full rettighet til å (1) trekke meg fra datainnsamlingen når som helst uten noen grunn, og (2) fjerne deler av eller all dataen som allerede er samlet av forskningsprosjektet uten noen grunn.

☐ Jeg forstår at gjennom prosjekt perioden og et år etter det (01.01.2022 - 31.05.2023), så vil den samlede dataen bli pseudonymisert. Jeg forstår at forbindelsen mellom pseudonymet og min virkelige identitet vil bli lagret separat og trygt beskyttet under NTNU sitt forskningsmiljø kun med hensikt for å ta kontakt ved data kvalitetssikring og for å oppfylle deltakernes rettigheter til tilgang, portabilitet og sletting.

☐ Jeg forstår at etter 31.05.2023 så vil all dataen samlet for dette forskningsprosjektet bli helt anonymisert i den forstand at det ikke vil være personlig identifiserbar informasjon som kan bli oppdaget fra den anonymiserte dataen. Jeg gir min tillatelse til forskningsprosjektets medlemmer til å få tilgang til og bruke disse anonymiserte dataene til oppfølgingsstudier.

☐ Jeg gir samtykke til at mine personopplysninger kan behandles frem til sluttdatoen for prosjektet, ca. 31.05.2022.

(Signert av deltaker, dato)

Software agents for enhancing privacy in homecare environment

Project Plan

by Abdurahman Godana and Runar Moen

NTNU
Norwegian University of
Science and Technology

1) Goals and Framework

1.1) Background

In recent years the concept of eHealth has become more relevant than ever before. While this has allowed for a lot of conveniences for both patients and providers, it has also created a whole new area of cyber security threats. It is very common to hear about data leaks in the medical field. A study performed in 2012 by the Ponemon Institute had found that 94% of hospitals had a security breach within the last two years, and furthermore 45% had experienced at least 5 breaches. While many practices have since been put in place to improve on this, there are still many security breaches and privacy concerns.

1.2) Project goals

The goal of this project will be to assess several security threats that come with electronic healthcare while also developing prototype software to mitigate them. The software agent will allow both healthcare providers and patients to configure their privacy settings and synchronize them, so that both the patient and the provider can choose whether to disclose sensitive information that would otherwise be unnecessary for the other party to know.

A provider may for example be able to request access to an electronic lock and predetermined times. If the patient also allows the provider access within their own software, the provider may get access as requested. If the patient denies this request, they will be given priority and the patient will not be given access. In cases where the provider is required certain privileges (e.g., the name of certain medications the patient is required to take), they will be given priority instead.

2) Scope

The context for homecare monitoring systems and assisted living technologies has some risks when it comes to privacy concerns. Therefor the aim of this thesis is what would we make better in use of those existing monitoring systems and assisted living technologies to help and protect patients and elderly privacies at homecare services based on their privacy attitudes and preferences. We will focus on designing an Android mobile app which will serve as a software agent for healthcare providers and patients to communicate and synchronize on privacy settings.

2.1) Subject area /problem specification.

Under this thesis the main tasks to be done is at first, we would understand the user requirement, identify each patient's own preferences that should be considered during homecare privacy design. Secondly, we will develop the Android APP based on these identified user requirements. Thirdly we should synchronize patients and healthcare privacy settings.

2.2) Methods and Delimitation:

The boundary of this thesis is patients and health care privacy setting under the homecare services. Different user requirements that are based on real scenario should be touched. The web app that would be designed based on patients and caregiver's preferences has focus on mind to minimize the privacy risks. During this work we should not include issues related to the health profession like medicine and medical treatments. The areas we consider are how to protect patients' privacy during homecare services. We consider cases like care services offered to target groups in living room, in activity areas and in common halls, and for instance, Care services given for peoples with disabilities under the cases of seizure and fall. Additionally, the thesis mission has determined time boundary.

2.3) Project Description:

The population aging in Norway has hit one million for the first time this year. This is the highest ever recorded number. Therefore, elders' homecare services using monitoring systems and assisted living technologies is a choiceless alternative. Among the advantages of the technologies made will help the elders to get medical help on time, reminding what time is it to take other daily routines. These includes some of the things they can do by themselves, gives signals and alarms in case the Severe incident like heart attacks and falling happens in living room, bathroom or sitting room in the absence of health care workers. A lot of research and industries has been done so far to help patients and elderly at home to get access to some basic activities. However, those technologies and systems have some limitations when it comes to patients' privacy setting. Even if many of the technologies has been introduced taking patients and elders privacy into consideration has help and protect them, but still remains security hole which exposed patient sensitive information into high risk. Still, more of the research is still underway to figure out and address each patient and elders' privacy preferences. Beside this, our focus in this thesis is to contribute to the setup individuals' privacy settings and behaviors while being monitored. Both technical staffs and health care providers should have to take patients privacy concerns into account while providing necessary assistants and providing medical help. Therefore, we should have to consider some of research questions and different scenarios while implementing assisting living technologies. One of the scenarios could be when a health care provider is scheduling a physical meeting with a patient, he/she should respect the patient's privacy preferences and get informed of that before a visit. A software agent allowing them to synchronize on privacy settings will help with the problem. Additionally, in this thesis we are going to design a mobile android app to serve as a software agent for health care providers and patients to communicate and make agreements on privacy settings.

2.4) Scientific Methodology.

- Create project plan.
- Reading resources to acquire more knowledge on thesis topics and relevant scenario.
- Identify user requirements and categorize different patient preferences at different aging level.
- Develop functional android app that will allow synchronization between patient and caregivers privacy.
- Synchronise patients and caregivers' preferences.
- Perform risk assessment.
- Testing products to gather customer feedback for further improvement.
- Writing project report.
- Prepare project presentation.

In summary, we intend to search relevant information to the scenario and use that as a baseline to develop our imaginary user requirements. This will mostly be based on various scientific research and data found from credible sources online and will all be cited in our final report.

3) Project Organization

3.1) Roles and responsibilities:

Under this category we assigned each other some specified roles and responsibilities for the project life span. Since we are a group of two members, we condensed the roles that might be used in a larger group to suit that of our own.

Team leader (Runar Moen)

Acts as point of contact with third parties.

Responsible for following up the project work activities.

Discuss with co-members and distribute workloads.

Responsible for how the overall project related works are implemented.

Ensure whether both members works jointly and independently if it is required.

Responsible for quality control for the reports or another document.

Quality control for the grammar or writing errors in reports.

Next leader (Abdurahman Godana)

Filling the leaders roll when leader is not available.

Act as the next point of contact for third parties.

Organize meeting and propose appropriate meeting time.

Responsible for archiving documents and submissions.

Ensuring all produced files are well documented and stored in the right place.

Responsible for collecting data and formatting of the final product.

3.2) Group Rules and Routines:

The group has agreed upon rules that have been established before the project starts. We are expected to uphold these rules to ensure that the project can be completed without issue. Here we describe our routines for regular meetings, our goals and ethics, and general rules and consequences for breaking them. In summary, we intend to

- We have scheduled regular meeting twice in every week where we will discuss and work together on the project. These meetings will be held on Wednesday and Friday primarily but may be changed if appropriate. Other meetings might occur if deemed necessary by the group.

- If problems arise, we will discuss it within the group and try to resolve it there. If no solution is found it will be discussed with the appropriate contact among the NTNU staff (e.g.
- Files will primarily be stored in Teams or Overleaf, but other solutions might be used if found appropriate and discussed beforehand in the group

We have also signed the NTNU Standard Agreement for student tasks. This document describes the rights of ownership over the project results, which will be held by the group members unless otherwise agreed upon.

4. Planning, follow-up, and reporting

4.1. Breakdown of main project work

For the success of our project, it is important to choose the right Software Development Life Cycle (SDLC). We have decided to use Scrum method in the Incremental Development Model. In the Software agent development we are going to communicate and synchronize the user requirements and preferences in homecare services.

- **Incremental Development model:** Is the most common approach which is appropriate for developing of application systems and software products. Since our thesis aims on creating some simple mobile app prototype based on user requirements.

Pros:

- Starting from the beginning of the project, users and other parties are all involved directly or indirectly by giving feedback throughout several versions until the required system is completed
- Consecutive feedback helps us achieve the expected product quality.
- It will be cheaper and easier to make changes under the development stage.
- We will be able to adjust the project as expectations of it change
- The most important user requirements are given high priority first
- It is possible for early delivery and deployment of important software for testing purposes

Cons:

- It requires a lot of planning
- Well defined module interfaces are needed.
- May require more resources
- More management attention required.

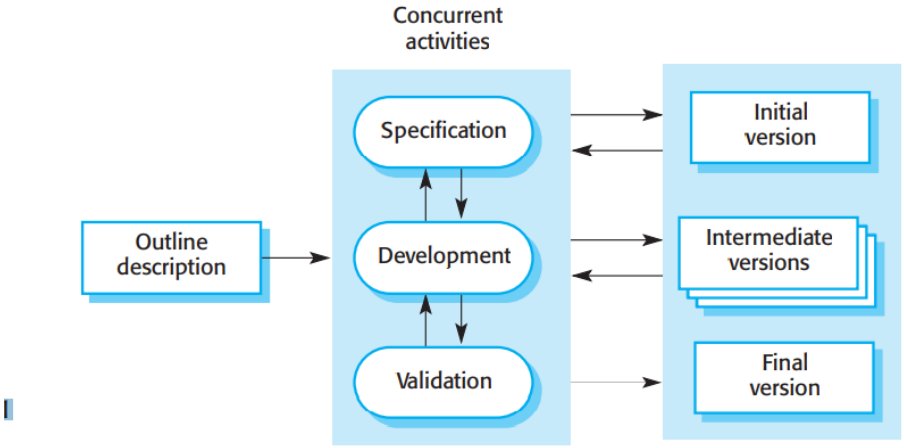


***Figure1**. **Incremental development**:- The Picture was taken from: Sommerville-Software-Engineering-10th-Edition, Chapter 2, page 50.*

- We plan on following the **Scrum method**. We will design an android mobile app prototype with appropriate user requirements. This model gives us good communication opportunities and flexibility in the development team. The model will ensure frequent partial delivery of expected product requirements to get customer feedback. By reflecting upon the different phases of the project, we can gain insight into how to continuously improve our work. The product is always responsive to changes and we will focus on working software that meets patient privacy negotiation.

4.2. Plan for meeting status and points of decision made in that period.

As previously mentioned, we intend to have meetings twice per week to ensure continuous progress during the project period. These meetings will act as our Scrum meetings. We are also looking to have regular meetings with the task giver, to know whether what we have produced at any given time can be up to the expectations set of us. During these meetings we will discuss the following:

- Progress made during the time between the last meetings
- What to do until the next meeting

We will also hold meetings with third parties, like our project advisor Guoqiang Li, or PhD student Luyi Sun. After each meeting we will write a short report detailing any important details discussed during the meetings.

5. Quality Insurance

5.1 Documentation, Standardization and Source Code

All sources used will be documented in the final report. This will include both dates and author. We will also credit teachers or other students that we might have received assistance from during the project period. If we end up using existing code or libraries for our software, it will also be credited in the project plan and the code itself.

We will use Bitbucket for version control of the software. This is to ensure that there is no conflicting code, and that each member can stay up to date on the project without any issues. The source code itself will be commented on regularly to ensure that it is readable and easily manageable by both the group and the examinators.

The final product will be publicly available on Bitbucket for the examination period, after which it might be taken down if agreed upon by the group. If other information (e.g version control logs) is needed for the examination of the project, it can be provided as needed.

5.2 Inspection and Testing

To ensure the quality of our project, we will perform regular tests on the software we produce. Tests will be done both manually by us and via automated test pipelines. The tests will mostly be focused on ensuring that the software is secure, and that there's no major bugs. We will also regularly proofread our final paper to ensure readability and clearness as we work on it throughout the project period.

5.3) Project Risks

In this section we will cover certain risks associated with our project and how we can potentially mitigate them.

We have identified **consequence values** for each risk as follows

High: Could severely affect the outcome of the project.

Middle: Could cause moderate issues with completion of project.

Low: Could cause short term or minor issues with the project.

Risk 1) Lack of time (Middle)

It is the first time our group has worked on such a large-scale project; it is important to realize that time might be an issue down the road.

Measure:

To ensure that this will not be a problem, we will have to work extensively on the project and make sure we reach the deadlines set by others and ourselves. Secondly, we should use our Gant-chart actively to follow up planned timeline.

Risk 2) Storage of data (High)

As the software we are developing deals with patient privacy, it is essential that we are careful with how we handle information. This also includes potential log-in information that the application would utilize.

Measure:

To resolve this, we must ensure we research methods of implementing features like data storage and login information thoroughly and use good industry practices. We also must research GDPR and other laws to ensure we are aware of what information we can store, and how to appropriately store it.

Risk 3) Vulnerabilities in Third Party Software (High)

There might be a scenario where a third-party software (e.g a database solution or an API) we decide to use contains some sort of vulnerability that can compromise the project.

Measure:

This can have potentially devastating and unpredictable risks and it is therefore crucial that we research whatever libraries or APIs that we decide to use, so we can make educated decisions on whether they are appropriate and safe for our project. We also need to ensure we are not using outdated software and are instead using the latest release when possible.

Risk 4) Errors in our own code (High)

Another concern is whether our own code will meet the expectations set of us Bugs or errors in the software code could be a serious concern that can leave us open to vulnerabilities or make the software unusable.

Measure:

To combat this, we must continually test our code and ensure to take in place good coding practices. While we do realize that we will be unable to fix every bug simply based on the time we have on the project, it is still important to try and get rid of as many as possible.

Risk 4) Internal Conflict (Low)

Internal conflicts in the group might always come up.

Measure:

To avoid this, we have work contract and scheduled regular meetings within the group to ensure that we agree before making changes or adding features. If this does not resolve the problem, we will have further routines for resolving conflicts.

Risk 6: Loss of documents (Low/Middle)

Occurrence of unwanted event that leads us to loss of document, may be missing the most important data.

Measure:

Have in place good back system in order to restore missing documents immediately. Therefore, we should realize consecutive backup taking manners both online and offline weekly or after each potential work progress permanently throughout project lifespan.

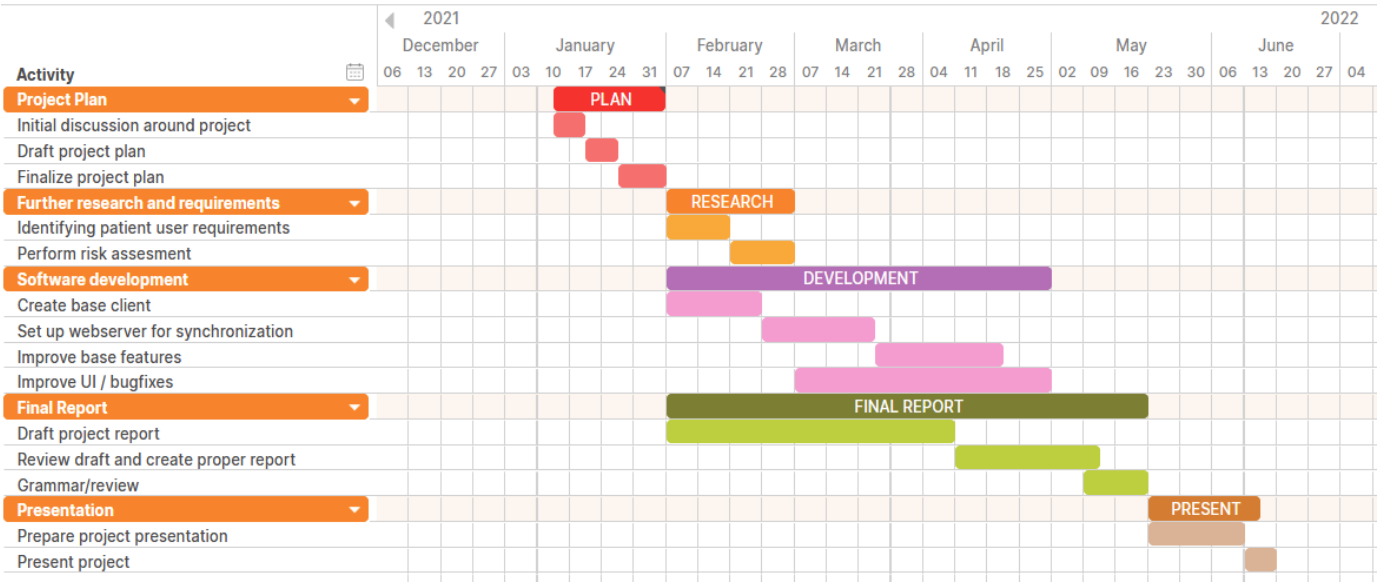
Risk analysis

The table maps different level of risk values from the perspective of consequences. Economy, confidentiality, reputation and privacy breach.

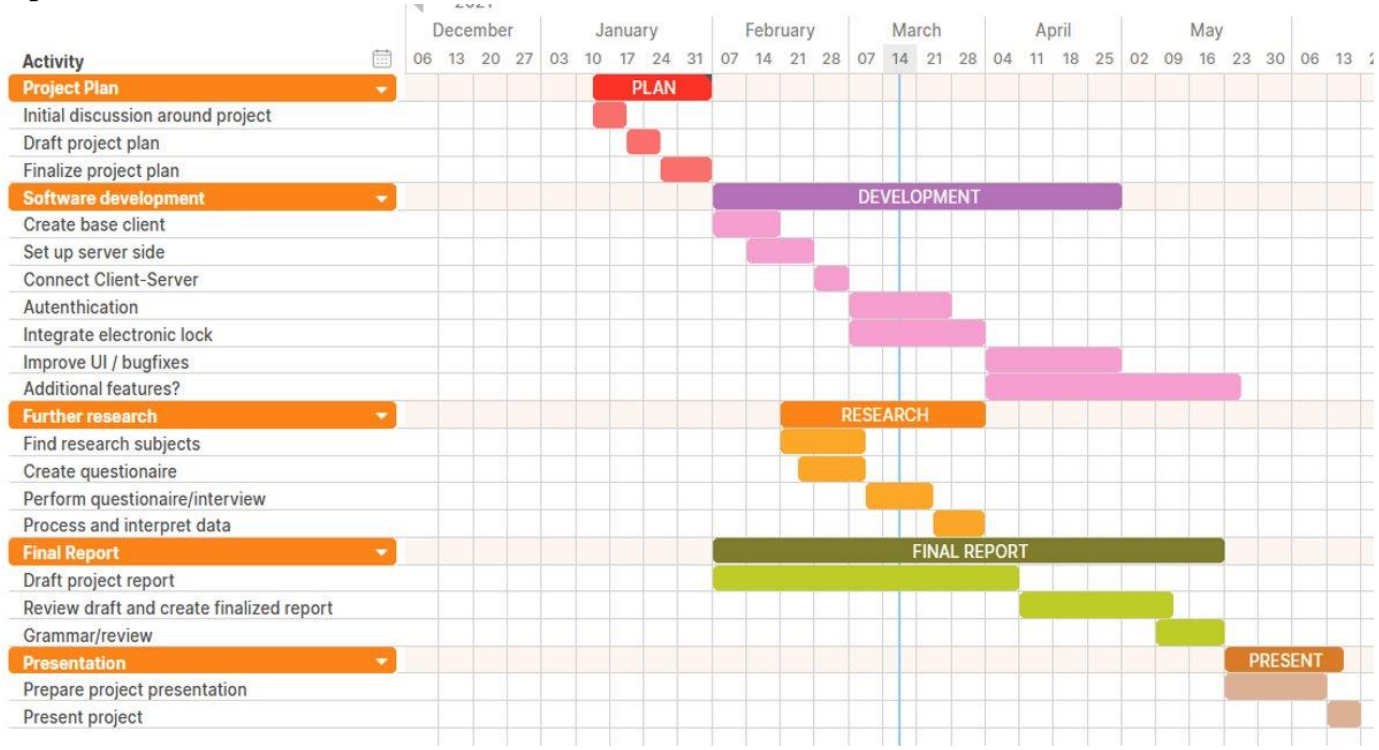
Consequences				
Consequence level	**Economy**	**Confidentiality**	**Reputation**	**Privacy breach**
High	Occurrence of Bugs or errors in the software code could be a serious concern that can leave us open to vulnerabilities or make the software unusable.	Serious problems which will damage our efforts and leads to project work failure.	Poor completion of project leads to it being perceived in a negative light or misunderstood by examinators.	Major bugs or vulnerabilities that could cause sensitive user data of many users to be compromised. Including, but not limited to: Login information or medical records.
Medium	Vulnerabilities in third party software that makes them incompatible with our own, forcing us to develop new software in its place.	Vulnerabilities in third party can affect directly or indirectly quality our project works.	Lack of plan B in case of failure and unable to discuss with project supervisor causes misunderstandings regarding on how project should be completed.	Major bugs or vulnerabilities that could cause the data of a smaller subset of user data to be compromised.
Low	Loss of important documents and data. Being unable to store different project versions phases and project data due to poor backup system.	Lack of version control routines and poor document storage manner will affect directly our project works.	Poor planning surrounding final presentation that causes project to be viewed in a negative manner by fellow students.	Minor bugs or vulnerabilities that affects few users, or exclusively include non-sensitive data (for example names, or phone numbers).
Insignificant	Inefficient use of time. Not able to use scheduled project work time in effective manner.	Minor data loss caused by software bugs, without any serious consequence for user.	Formatting errors in final report gives it an unprofessional look among examinators.	Minor loss of data that could cause small inconveniences for a subset of users.

6) Implementation plan

In the Gantt below we give an overview of how we intend to follow through with our project. We have separated it into five stages: the planning phase, the researching phase, the development phase, the reporting phase and the presenting phase. These phases are themselves separated into smaller phases that we will continuously work on throughout the project. We are currently in the planning phase.



Updated Gantt:



❖ Milestones and Decision points.

These are the

Milestones:

- Ensure thesis work to meet expected outcomes. ----------by 20.04.2022
- Pass the thesis work. ---------- 10.06.2022
- Submitting the functional thesis work which will contribute additional findings for the field research. ----------20.05.2022
- Presentation of the findings/thesis for partners and schools. ---- 07.06.2022

Activities:

- Write and review final thesis
- Collect information and resources to acquire more knowledge on scenario.
- Define research scenario
- Create project environments on bitbuckets.org (clients and server side).
- Identify user requirements.
- Understand and categorize different patient preferences in line with elderly category.
- Develop android app that will allow synchronization between patient and caregivers privacy.
- Synchronise patients and caregivers' preferences.
- Generate complete reports.
- Prepare project presentation.

Sources:

All sources were last accessed and validated as of 29.01.2022.

- https://www.ponemon.org/local/upload/file/Third_Annual_Study_Patient_Privacy_FINAL.pdf.
- https://www.researchgate.net/publication/282280458_Big_Data_Security_and_Privacy_Issues_in_Healthcare.
- https://www.pearson.com/us/higher-education/program/Sommerville-Software-Engineering-10th-Edition/PGM35255.html.
- https://bitbucket.org/bachelorntu2022/bachelor-2022/src/master/ (Project reposotory)

Images:

- https://ntnu.app.box.com/v/logoer-ntnu-diverse/folder/93813255503
- https://freesvg.org/caring (
- https://uxwing.com/safe-icon/
- https://plan.tomsplanner.com (Gantt)
- *Incremental development, Sommerville-Software-Engineering-10th-Edition, Chapter 2, page* 50.

Bibliography

[1] D. for e-helse, 'Innbyggerundersøkelsen om e-helse 2021,' *ISBN-10*, 2021.

[2] Norwegian Labour and Welfare Administration, *Nå har Norge én million pensjonister*, [Online; accessed 18-May-2022]. [Online]. Available: %7Bhttps://www.nav.no/no/nav-og-samfunn/statistikk/pensjon-statistikk/nyheter/na-har-norge-en-million-pensjonister%7D.

[3] I. Sommerville, 'Software engineering 10th edition,' *ISBN-10*, vol. 137035152, p. 18, 2015.

[4] J. vom Brocke, A. Hevner and A. Maedche, 'Introduction to design science research,' in *Design Science Research. Cases*, Springer, 2020, pp. 1–13.

[5] C. Pang and A. Hindle, 'Continuous maintenance,' in *2016 IEEE International Conference on Software Maintenance and Evolution (ICSME)*, IEEE, 2016, pp. 458–462.

[6] E. Thorstensen, 'Privacy and future consent in smart homes as assisted living technologies,' in *International Conference on Human Aspects of IT for the Aged Population*, Springer, 2018, pp. 415–433.

[7] A. Casamayor, D. Godoy and M. Campo, 'Identification of non-functional requirements in textual specifications: A semi-supervised learning approach,' *Information and Software Technology*, vol. 52, no. 4, pp. 436–445, 2010.

[8] Oracle, *Java™ Platform Overview*, [Online; accessed 12-May-2022]. [Online]. Available: %7Bhttps://docs.oracle.com/javase/8/docs/%7D.

[9] Platform Architecture, [Online; accessed 12-May-2022], 2022. [Online]. Available: %7Bhttps://developer.android.com/guide/platform%7D.

[10] Tim Lindholm, Frank Yellin, Gilad Bracha, Alex Buckley, *The Java® Virtual Machine Specification*, [Online; accessed 12-May-2022], 2015. [Online]. Available: %7Bhttps://docs.oracle.com/javase/specs/jvms/se8/html/%7D.

[11] L. Junyan, X. Shiguo and L. Yijie, 'Application research of embedded database sqlite,' in *2009 International Forum on Information Technology and Applications*, IEEE, vol. 2, 2009, pp. 539–543.

[12] Wikipedia contributors, *Garbled circuit — Wikipedia, the free encyclopedia*, [Online; accessed 11-April-2022], 2021. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Garbled_circuit&oldid=1061953217.

[13] A. C.-C. Yao, 'How to generate and exchange secrets,' in *27th Annual Symposium on Foundations of Computer Science (sfcs 1986)*, 1986, pp. 162–167. DOI: 10.1109/SFCS.1986.25.

[14] *Project repository (BitBucket)*. [Online]. Available: %7Bhttps://bitbucket.org/bachelorntu2022/bachelor-2022/src/maste/%7D.

[15] *Project repository (GitLab)*. [Online]. Available: %7Bhttps://git.gvk.idi.ntnu.no/runarmon/bachelor-2022/%7D.

[16] Wikipedia contributors, *Software testing — Wikipedia, the free encyclopedia*, [Online; accessed 28-April-2022], 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Software_testing&oldid=1083360797.

[17] Wikipedia contributors, *William c. hetzel — Wikipedia, the free encyclopedia*, [Online; accessed 28-April-2022], 2019. [Online]. Available: https://en.wikipedia.org/w/index.php?title=William_C._Hetzel&oldid=885753650.