INSTALLATION AND TESTING OF TECHNICAL DEVICES AND APPLICATIONS

Deliverable D.T3.7.4

Final version

04 2021

Table of contents

1. Introduction

The Monitoring Grid was developed in the present project as part of Working Package T2 “The design and development of technical solutions”. It is a web application and acts as a simple monitoring tool, which shall enable a monitoring team to detect early signs of deterioration of health and social conditions and consequently enable older people to live independently at home as long as possible. In this respect, it represents the basis for weekly calls. These calls serve to identify a deterioration in mental and physical health as quickly as possible. This means, it not only pursues the goal of recognizing a deterioration in the state of health as quickly as possible, it also intends to manage and facilitate phone interviews with frail elderly people, thus constituting a true "guide" to handle phone interviews.

In addition to the weekly calls that elderly people receive from a trained monitoring team, they also have the option of contacting the monitoring team themselves if they want to, e.g. if they have important questions. To make this possible, another button, the so-called service button[1], was activated for the already existing home emergency call. When the elderly press this button, they are connected directly to the interviewer assigned to them.

As part of the project, the target group of the pilot action was adapted to the actual priorities and circumstances of the Samaritan Burgenland Department of Home Care. Since the living environment (private homes, homes of assisted living), in which the service button is activated, naturally depends on the target group, the adaptations of the target group are first briefly described. In the next step, important technical properties and security aspects, as well as the requirements for a system that wants to install the Monitoring Grid are described. It then briefly describes how the Samaritan Burgenland Department of Home Care installed the Monitoring Grid and tested it before the start of the pilot action. The last point deals with the activation and testing of the service button on the home emergency call devices.

[1] Service button = Service Taste in German

2. Modifications

As already described in detail in "D.T3.7.2 Engagement of test persons and consideration of legal aspects", there were changes in the target group:

Target group	Reason for selection of the target group
Persons,	
1. who are older than 75 years old,	Age: This criteria is based on the Monitoring Grid in Bologna
2. live in Burgenland, and	Region: In middle of Burgenland we have too few residents in homes of assisted living and too few home emergency call users. For this reason we have expanded the target group to entire Burgenland.
3. who have a home emergency call, which can be expanded to include the service button.[2]	Use of home emergency call: In the needs analysis, which was carried out in WP T1, it turned out that possible participants also want to have the opportunity to contact the monitoring team. For this reason, this criterion has been added, but it is not mandatory to meet it.

Table 1: Description of the changes in the target group.

According to these changes, the service button was not only installed in homes of assisted living in Middle Burgenland, as stated in the application form (*„Installation of technical devices and applications in Home of assisted living in Mittelburgenland…")*. Rather, they were installed in private houses and homes of assisted living throughout Burgenland. The following table briefly shows where the activation/ installation of the service button and the testing of their functionality took place. As can be seen from the table below, participant number 9 does not have a home emergency call. Accordingly, there was no activation of the service button on the home emergency call device:

[2] Note: Not all home emergency calls can be expanded to include an additional button. The mobile devices, for example, do not have this option.

Participant number	Sex	Year of Birth	NUTS Region	Living conditions	Home emergency call	Date of installation
1	female	1934	111	alone	Yes	09.02.2021
2	female	1945	111	alone	Yes	09.02.2021
3	female	1940	112	alone	Yes	09.02.2021
4	female	1933	111	alone	Yes	10.02.2021
5	female	1938	111	alone	Yes	10.02.2021
6	female	1939	112	alone	Yes	11.02.2021
7	female	1936	111	with her daughter and son in law	Yes	15.02.2021
8	female	1935	111	alone	Yes	15.02.2021
9	female	1941	111	alone in an assisted living home	No	15.02.2021
10	female	1935	111	alone	Yes	15.02.2021
11	female	1937	113	alone in an assisted living home	Yes	17.02.2021
12	female	1936	113	alone in an assisted living home	Yes	17.02.2021
13	female	1935	112	alone	Yes	17.02.2021

Table 2: List of where the activation of the service button on the home emergency call took place.

3. Installation and testing of Monitoring Grid

The Monitoring Grid was jointly developed by PP8 (Samaritan Burgenland Department of Home Care) and PP2 (Brno University of Technology). PP8 developed the concept for the Monitoring Grid in cooperation with the residential area managers of the Samaritan Burgenland Department of Home Care. PP2 organized the technical implementation.

After the technical implementation of the Monitoring Grid was completed at the end of December 2020/ beginning of January 2021, the transfer of the Monitoring Grid for the pilot action, in which the functionality of the Monitoring Grid will be tested, had to be prepared from PP2 to PP8. In the following, the requirements for a successful takeover are presented. In addition, you will find an installation guide in the appendix, which should make it easier for the user to install the Monitoring Grid on his systems.

3.1. Description of the requirements for a successful installation

Before describing what requirements, the "user" system must have in order to be able to successfully take over the Monitoring Grid, some important technical properties of this web application and security aspects are briefly described.

3.1.1. Application requirements

The technologies used to develop the Monitoring Grid tool arose from several requirements, including interactive web interface, data security, permanent data storage, scalability, and consideration for future expandability. Based on the mentioned requirements, Framework Spring has been chosen. It provides a comprehensive programming and configuration model for modern Java-based enterprise applications - with any kind of deployment platform[3]. A relatively crucial issue is also the ability to relatively easily deploy the

[3] "Spring Framework," Spring. [Online]. Available: https://spring.io/projects/spring-framework.

developed application to the customer's servers. The ideal solution is to deliver the information system in the form of an executable package that is configurable through the attached file. It has been necessary to create stand-alone Spring based Application, thus Spring Boot has been chosen. In addition, several other technologies have been used for development, for example:

- Spring Boot 2.3.3
    - Spring MVC
    - Spring Security
    - Spring Data JPA
        - Hibernate 5.4.20
- Thymeleaf 3.0.11
- Bootstrap 4.4.1
- JavaScript
    - jQuery 3.4.1
        - AJAX
- Open-source third party libraries
    - Tempusdominus Bootstrap 4 v.5.1.2 - MIT license
    - Select2 v.4.0.13 - MIT license
    - iCheck v.3.0.1 - MIT license
    - ChartJS v.2.9.3 - MIT license
    - AdminLTE v.3.0.5 - MIT license
    - Datatables v.1.10.20 - MIT license
    - Daterangepicker v.3.0.5 - MIT license
- PostgreSQL
    - DB 9.6.21
    - Automatic backup script
- WinSW
    - NET Framework 3.5

3.1.2. Application architecture

There are a number of software architectures according to which information systems are designed, namely HMVC, MVVM, MVP, MVA and the like. In the case of the Monitoring Grid, the Model-view-controller (MVC) software architecture was used. It is a software architecture that divides the application data layer, presentation layer, and business layer into three independent components so that modifying some of them has minimal effect on others. The architecture of the Monitoring Grid is composed as other similar applications of layers including:

- Presentation layer (user interface) – Displays information to users, usually in the form of a graphical user interface, which can control input, but does not include data processing.
- Business layer - the core of the application, contains logic, functions and data processing.
- Data layer - This layer most often consists of techniques arranging object-relational mapping. It is basically a programming technique that provides automatic data conversion between a relational

database and an object-oriented programming language. Furthermore, with its use it is possible to create database queries. Their purpose is to store, delete, modify and read data in the database.

3.1.3. Spring flow architecture

The flow architecture represents a slightly more detailed awareness of the interconnection of the layers occurring in the MVC with the relational database. Figure 1 shows the data flow between the individual layers in the Monitoring Grid as well as the communication between the client, and the server where the information system is running.

1. The Monitoring Grid client sends requests to one of the existing end-points that are mapped in the controller. Note that the using so-called endpoints, there is an interaction between the user and the server application in which they are defined. Each endpoint is designed to fulfill some specific purpose, such as logging in, displaying interviewee (elderly) information, and so on. The requests can contain one or more parameters, i.e. login credentials, interviewee ID for which the client wants to display information, etc.
2. In the endpoint which is defined in the controller are performed some operations. A typical example is, first of all, verifying the client's credentials or the validity of his session. If any parameters have been sent in the request, they are extracted and then passed to the defined method in the next layer.
3. The service layer should, in essence, handle most of the computational operations and logic that calls the appropriate methods in the DAO layer.
4. The DAO layer is in charge of interacting with the database. This is where operations occur that aim to transition between an object-oriented and a relational view. Parameterized database queries are created here based on the parameters passed from the previous layer. Also important is the link with the model, which is shown in blue in Figure 7. Entities (objects) and truths are defined in the model, most often by means of notations, for conversion between objects and relations. Operations performed in the DAO layer can be of 2 basic types:
    a. Read - maps a relational structure to objects
    b. Write - maps objects to a relational structure

    A typical case of a read operation is an attempt to obtain information and bindings of one or more objects (interviewees, user, interview, etc.), to obtain the number of stored entities, or to search in a huge amount of data. Write operations are mainly used to persist new entities, to modify them or to permanently delete them from the database. Based on the purpose of the operation performed in the DAO layer, information may be returned to the previous layer. These can include primitive data types and objects (either separate entities or a collection of entities).
5. If the method in the service layer is already completely executed, it returns to the place from which it was called, i.e. to the appropriate endpoint in the controller. The relevant endpoint has the same option. You can also call multiple methods in multiple service layers.
6. As soon as all the required operations are performed and the required data is obtained from the database, a so-called view is created on the basis of them. It is then sent in response to the client.

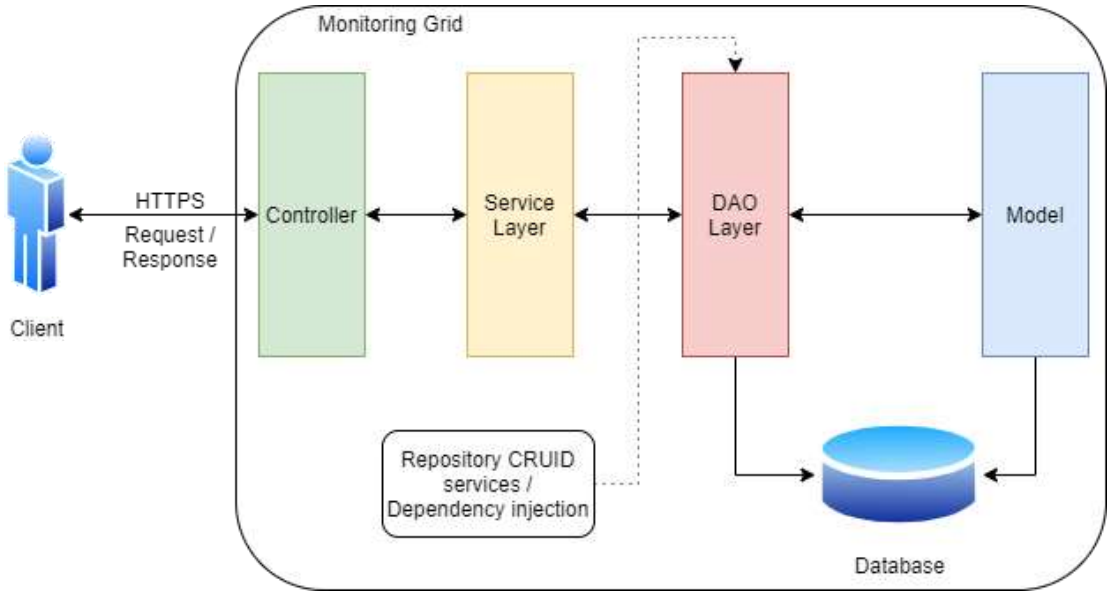

Figure 1: The Monitoring Grid flow architecture.

3.1.4. User hierarchy

A hierarchical model of user accounts was designed to meet the required functionalities and capabilities of the Monitoring Grid information system.

- Administrator account - only one, permissions:
  - create the interviewer's account,
  - create account to interviewees,
  - change the passwords of all accounts,
  - add new interviewees,
  - edit interviewees detail,
  - delete interviewees,
  - create interviews with elderlies,
  - show interviews, comments, answer combinations.
- Interviewer account – unlimited number of this account type, permissions
  - add new interviewees,
  - delete assigned (own) interviewees,
  - create account to assigned (own) interviewees,
  - edit interviewees detail,
  - create interviews with elderlies,
  - show interviews (only of assigned), comments, answer combinations
- Interviewee's account - an unlimited number, permission:
  - change own details,
  - show interviews (only his own), comments, answer combinations,
  - change his password.

3.1.5. Security

In the development of information technology, there is also an attempt to misuse these resources, for example to gain access to confidential data. It is therefore necessary to apply certain techniques in the proposed information systems that increase safety. One of the most important factors is the use of the HTTPS communication protocol, which uses the HTTP protocol in combination with the TLS cryptographic protocol. The purpose of the HTTPS protocol is to transfer encrypted data between the client and the server. This encrypted data can be intercepted by a hacker, but cannot be decrypted in a reasonable amount of time without knowing the encryption keys. The process of establishing a connection between the client and the server is shown in Figure 2.

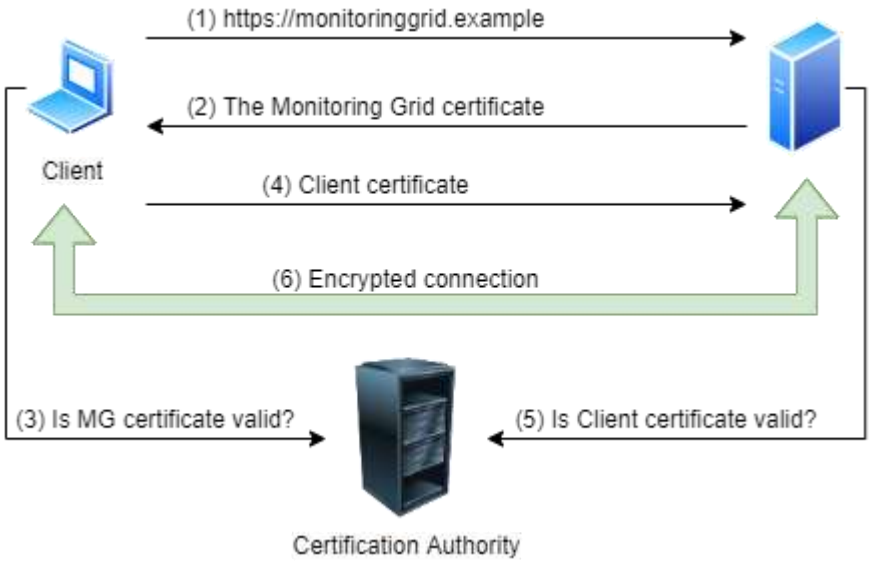

Figure 2: Establishing a secure connection between the client and the server.

Using only an encrypted connection is not enough. It is necessary to ensure access to the Monitoring Grid only to persons who are authorized to interact with the server application. This is achieved by knowing the username of secret information - passwords. Based on this information, it is verified whether the currently logged in client is who he pretends to be. For this reason, the following the Monitoring Grid login mechanism has been implemented (Figure 3):

1. the client fills the credentials and sends login request to the server,
2. the endpoint defined in the Login Controller invokes the method in the *Security Util* class and passes the extracted login credentials from request,
3. Based on the result of the method *already Logged:*
    a. if the session is a valid, the user is already logged, return login success,
    b. based on the username, the persisted user account is read from database,
        i. compute hash of the password sended in the request together with the salt of the found account,
        ii. check if the computed hash is the same as the persisted password. If true, return login success and create a valid session, else return bad credentials error.

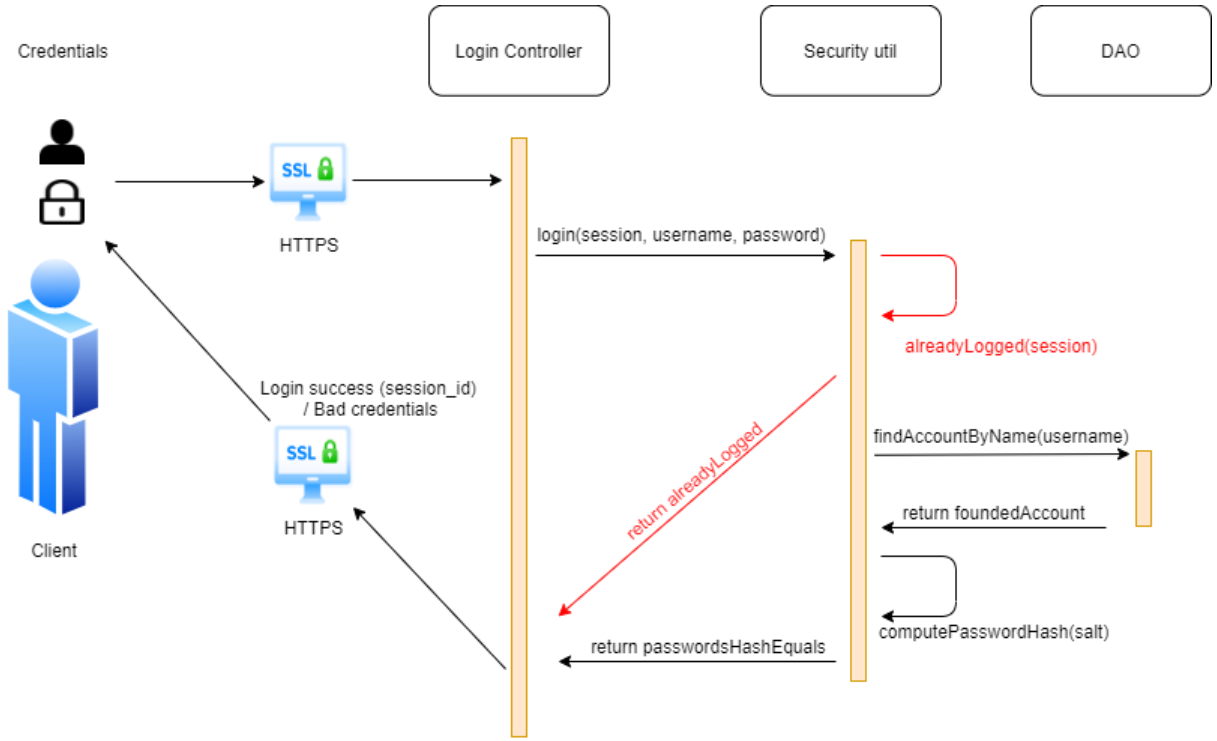

Figure 3: Pipeline of verifying the client's login credentials.

There are several types of user accounts in the Monitoring Grid that primarily differ in what operations they can perform. The Monitoring Grid information system processes confidential personal data of interviewed elderlies and it is therefore necessary to create a mechanism that will allow access to this data only to authorized users. For this reason, logic is implemented in the application to determine what operations a type of user account can perform. Figure 4 shows a flowchart of a method that decides whether to deny or allow an operation.

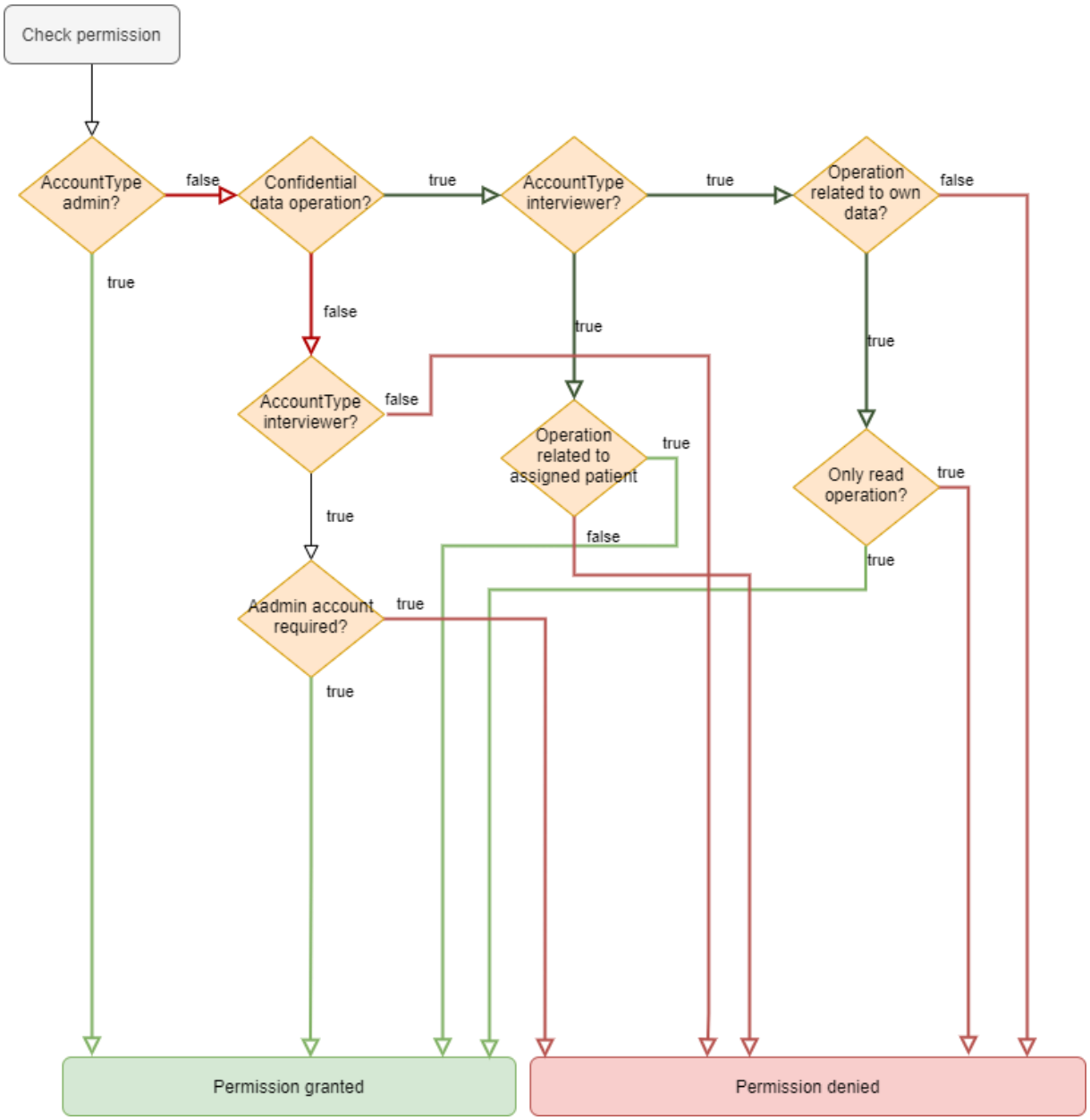

Figure 4: Flowchart of the permission method. The operation that the user wants to perform is denied or granted.

Increasing the security of the Monitoring Grid is also achieved by disabling public registration of new user accounts. These can only be created by an authorized person holding an administrator account or an interviewer account. Each user account must meet the minimum password requirements:

- at least one upper letter,
- at least one lower letter,
- at least one number,
- at least 8 characters.

For security reasons, storing passwords in the database unchanged cannot be accepted. The solution is as follows:

1. The client fills in an username and password that meets the required security features and send a request;
2. a random sequence of bytes is generated, and this sequence is stored in a new Account entity;
3. hash by SHA-512 hashing function of entered password together with salt is calculated;
4. the hash is stored in a new Account entity in *password* attribute.

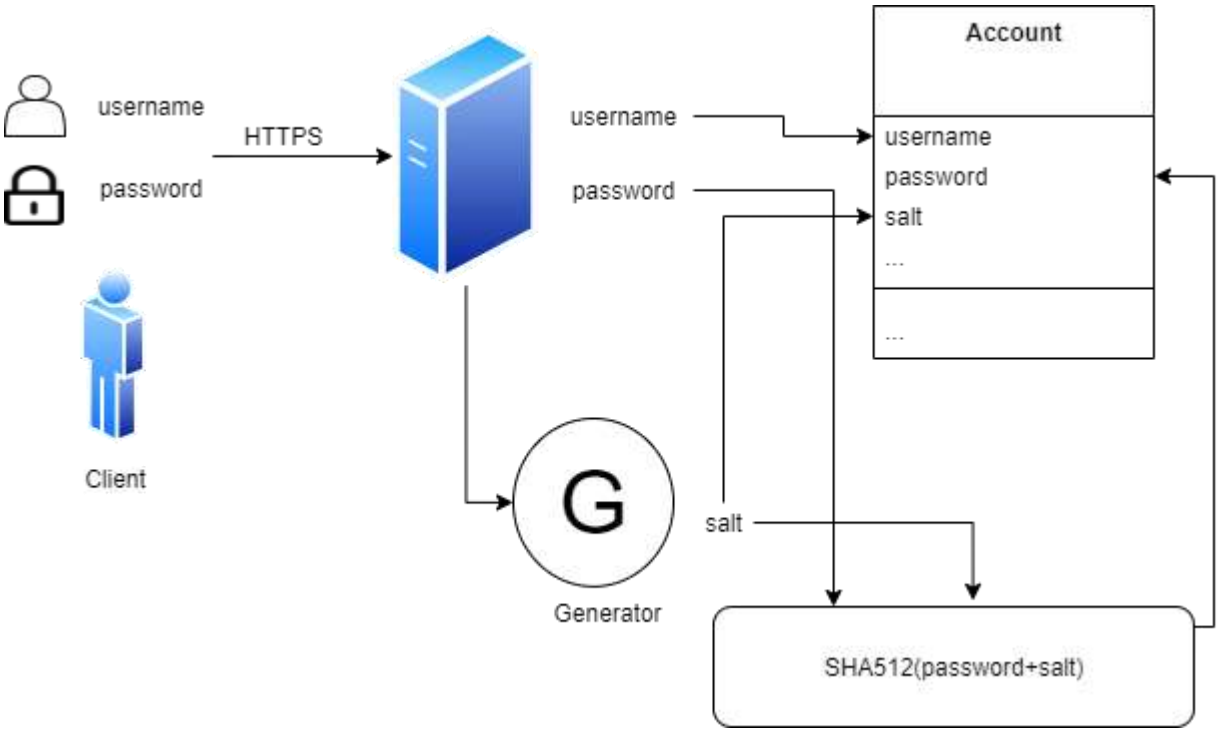

Figure 5: The process of registering a new user account - specifically the part dealing with secure password storage.

3.1.6. Server-side data table processing

The Monitoring Grid contains several tables that show, for example, existing interviewees, their interviews, a list of users, and the like. The amount of this data can grow rapidly, and if the correct approach is not chosen, the application would gradually and significantly slow down. This situation would occur if all data were loaded at the time of creating the view in the server application. Loading data into tables and their subsequent searching is performed by so-called asynchronous JavaScript (AJAX) requests. This is a so-called server-side approach (Figure 6). First of all, a page is rendered to the user in a web browser, and in the meantime another query is sent to the server, which contains many parameters, such as page size, search term, current page number, and so on. The advantage is that in the case of a large number of records, it is not necessary to load all data during page rendering. This reduces the time required to process a user query.

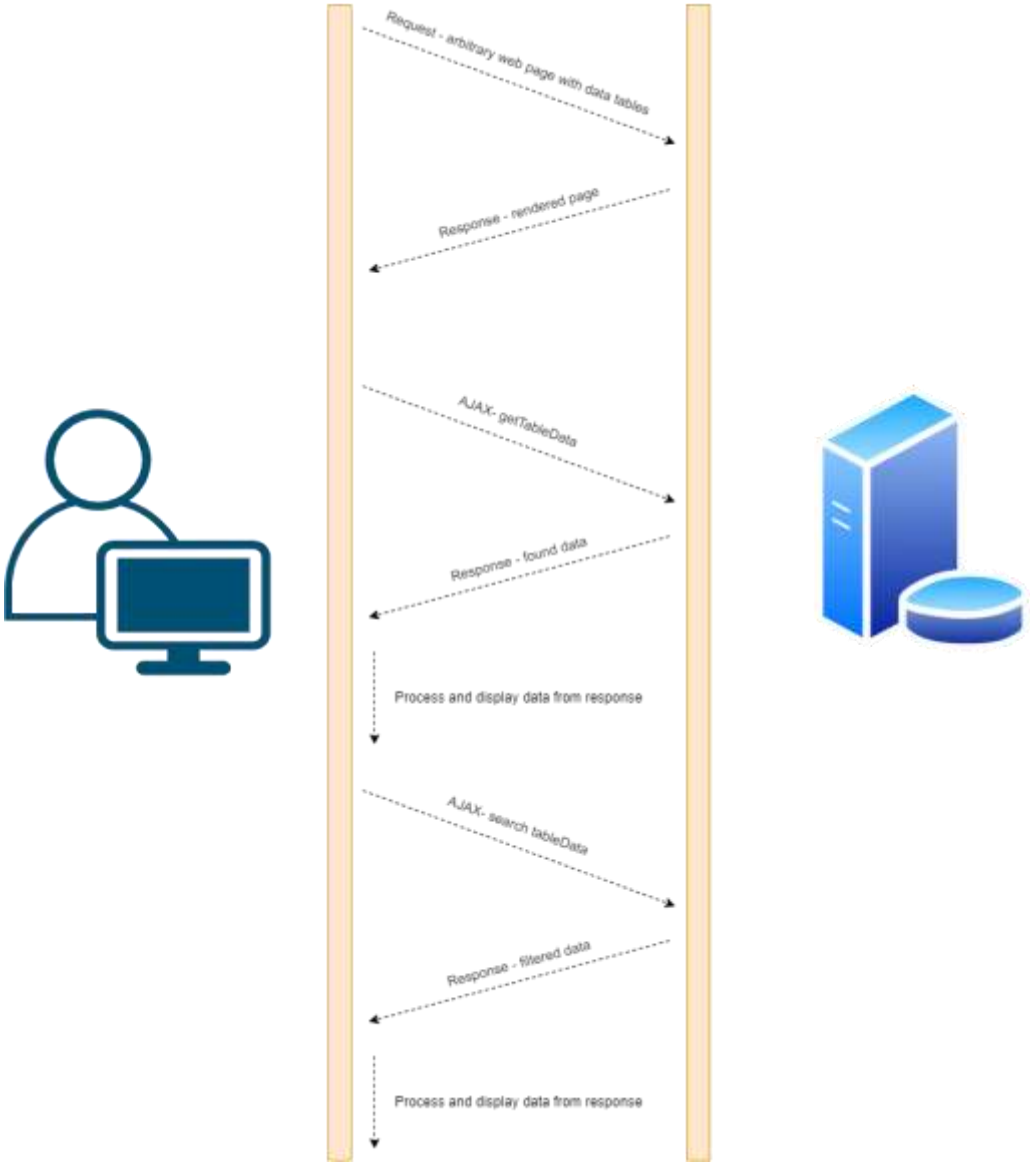

Figure 6: Simplified example of the communication between the server and the client in the case of using server-side datatables processing.

3.1.7. Data model

Data modeling is one of the disciplines of software engineering. It is a process in which the requirements for the data structure used by the information system are defined and analysed. The result of this process is a data model. Data models describe (define) the format and structure of data in these systems and determine the interrelationships of individual data elements with each other, thereby representing a defined part of reality. This allows us in the resulting system to manipulate this data and use it for the purpose for which it was entered into this system. A simplified data model that is used in grid monitoring can be seen in Figure 7. There are several basic classes that define the system as a whole. The most important object within the monitoring grid is the administrator account, which can associate several interviewer accounts or interviewees directly. A maximum of one "elderly" account can be assigned to one elderly. It ensures that the elderly is informed about all entered and existing data in the Monitoring Grid. There can be a number of interviews for each elderly. These contain stored information about the interviewee's answers to certain types of questions. Based on them, it is then possible to generate a

graphical representation of the interviewee's condition, or to display all comments or resulting combinations of answers.

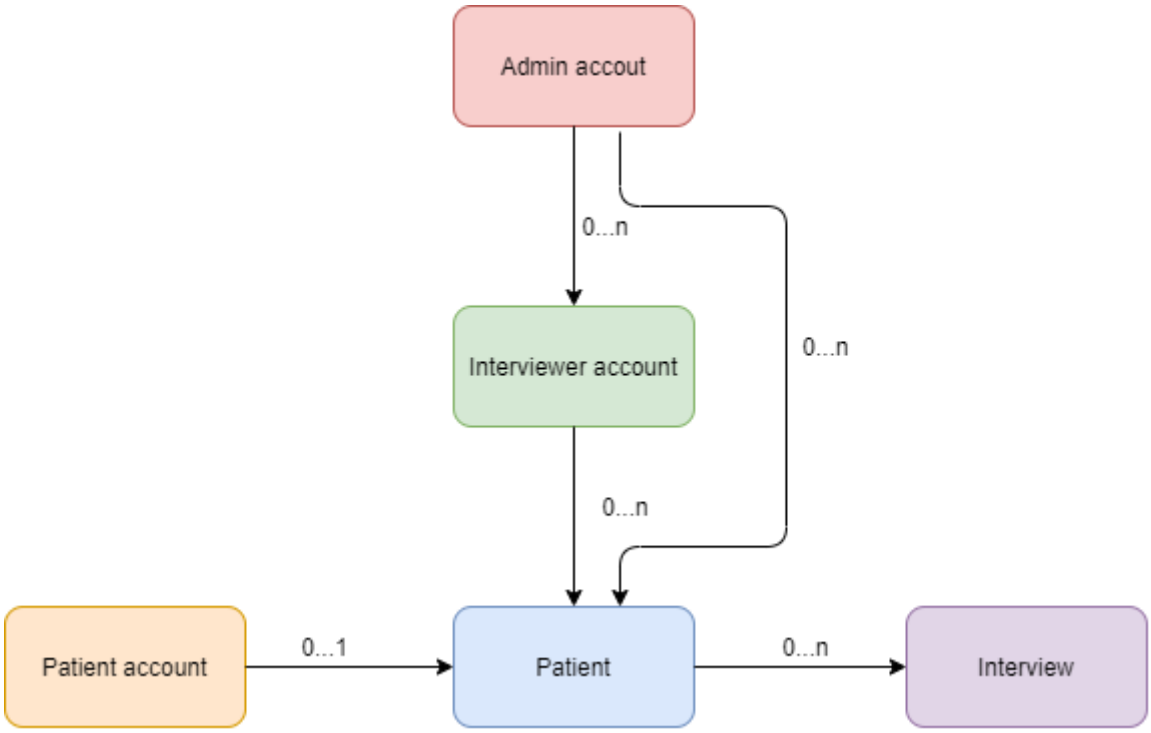

Figure 7: Simplified data model used in the Monitoring Grid application.

3.1.8. System requirements

To take full advantage of all the proposed parts of the Monitoring Grid and its correct start-up, it is necessary to meet several minimum system requirements, including:

- Hardware:
  - CPU: Quad-core 2,5 GHz
  - RAM: 8 GB
  - HDD: 128 GB
- Software:
  - OS: Windows or Linux
  - JAVA 8 or newer
  - PostgreSQL database 9.6 or newer
  - SSL Certificate

3.1.9. Database backup and Windows autorun service

Complete data loss is the biggest threat in the operation of any information system. It can be caused by a hardware failure, a hacker attack, a serious system error, in exceptional cases, an operating system update, or a human error. The only way to avoid a scenario with very strong negative effects is to back up regularly. It is recommended to run the script regularly according to your organization's policy (every n hours / days / etc.) and automatically (e.g. by Windows Task Scheduler). It is also recommended storing backups in

multiple independent locations (the server where MG runs and some other physical storage). In the event that one of the above-mentioned situations occurs, only data will be lost for the maximum length of the backup interval.

The maximum availability of the Monitoring Grid was decided to use tools in order to create a service that takes care of its automatic start. In the event of an accidental restart of the server or a power failure, the start-up and thus the availability of the Monitoring Grid together with the Windows operating system is guaranteed. Windows Service Wrapper – WinSW is used for wrapping the executable JAR file, which has been created by Spring boot, as a Windows service. Using the WinSW, a tool has been created to start the Monitoring Grid every time the server is started, thus ensuring the availability of the service.

3.2. Installation and testing in the user's system

In order to be able to use the Monitoring Grid at the Samaritan Burgenland Department of Home Care, it was first important to prepare a virtual server with Windows operating system. The developer's (PP2, Brno University of Technology) software was installed on this Windows server. The installation was carried out according to the installation guide prepared by PP2, which can be found in the appendix.

Authorizations are assigned directly in the application and there are corresponding admin users in the area of the Samaritans Austria. [4] The IT department has no user to administer the software and no read access either. After completing the setup, a backup job was also created according to the instructions of the developer. In addition, the entire server with all settings is backed up daily at night. A retention period of two weeks has been defined for the backups. The software developers maintain and update the software. A corresponding maintenance contract between PP2 and PP8 has been prepared for this purpose. In the event of malfunctions or failures, the IT department rectifies the problem with appropriate escalation to the software developer.

Before the pilot action started in April 2021, fictitious interviews were entered in the Monitoring Grid. On the one hand, these were used to test the functionality of the monitoring grid in advance and, on the other hand, they were also used at the same time to train the interviewers in order to be able to explain the functionality of the monitoring grid to them.

4. Installation and testing of the home emergency call

In February 2021, the project management and the person responsible for the home emergency call visited the participants in their personal living environment (at home, homes of assisted living). During these visits, care was taken to comply with the Covid-19 requirements applicable at the time and to protect the privacy of the participants as much as possible. In addition to comprehensive project information and handling of all formalities (declarations of consent, data protection, ...), the service button was activated on the already existing home emergency call. The original purpose of the home emergency call is to be able to call the ambulance in an emergency by pressing a single button.

The now activated service button enables the participants, in addition to the weekly calls, to contact the monitoring team or the interviewer assigned and to ask them questions, which are important for the participants. Times have been set for this, namely Monday to Friday from 9:00 a.m. to 12:00 p.m.

Depending on the device, it is either a yellow or a green button (in Picture 8 it is the yellow, in Picture 9 the green button).

[4] Note: Samaritan Burgenland Department of Home Care is a subsidiary of Samaritan Austria. The IT, which is employed by the Samaritan Austria, is also responsible for the subsidiaries.

Picture 8: Person responsible for the home emergency call labels the device with "SERVICE TASTE".

Picture 9: Device is labelled with "SERVICE TASTE" (= service button).

The buttons on the devices can be activated and programmed in a user-defined manner. The telephone number of the respective interviewer was programmed as part of the project. By pressing the service button on the device, the interviewees are immediately connected to "their" interviewer and the integrated hands-free facility enables the interviewer, and the person being interviewed to talk straightaway.

There are the following differences in the installed devices:

- Devices that are operated via the fixed network (alarm transmission and calls with the service button are handled via the fixed network). These devices require an active landline connection - this is provided by the customer.
- Devices that are operated via the GSM network (alarm transmission and calls with the service button are handled via the GSM network). These devices require an active SIM card for the GSM network - this is provided by the Samaritan Burgenland Department of Home Care. Two years ago the manufacturer changed the production of devices and developed a new design. Therefore, different devices are used here (the "old" devices as well as the "new" devices). On the old devices the service button is yellow, on the new devices the service button is green.

After activating the service button, the home emergency call offered by the Samaritan Burgenland Department of Home Care therefore will have two active buttons, each of which has one function:

1. Contact option for rescue in the event of an emergency (= emergency button, current function).
2. Opportunity to contact the monitoring team to ask essential questions (= service button, new function).

After the service button was linked to the telephone number of the respective interviewer, the person responsible for the home emergency call tested the functionality. This was handled by actively pressing the service button and checking the connection between the home emergency call device and the interviewer. There were no problems with eleven of the twelve installed service buttons. With one emergency call device the connection could not be established. However, after consulting the manufacturer of the devices, the problem was solved.

5. Conclusion

As part of Working Package T3 “Pilot testing of technical solutions and health and care models”, the Monitoring Grid developed in Working Package T2 is tested. This document describes the transfer of the Monitoring Grid from the technical developer of the web application (PP2, Brno University of Technology) to the user/ tester of the web application (PP8, Samaritan Burgenland Department of Home Care). In particular, the most important technical properties, essential security aspects and the requirements for a system that wants to take over the Monitoring Grid are described.

The Monitoring Grid is supported by the in this project activated service button of the home emergency call. Pushing the so-called service button enables older people to contact the monitoring team themselves, if they want to. The installation process and testing of the service button are also described.

The process of taking over the Monitoring Grid and activating/ installing the service button on the home emergency call did not cause any problems. Only in the case of one home emergency call no connection could be established between the interviewer and the interviewed person. However, after consulting the manufacturer of the devices, the problem was resolved.

6. Appendix

1. Installation Guide Monitoring Grid