Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

A Solid-Powered Collaborative Rule Management Tool for Sharing Patient Data

Lokesh Selvakumar

A Dissertation

Presented to the University of Dublin, Trinity College

in partial fulfilment of the requirements for the degree of

Master of Science in Computer Science (Intelligent Systems)

Supervisor: Dr David Lewis

August 2022

Declaration

I hereby declare that this dissertation is entirely my own work and that it has not been submitted as an exercise for a degree at this or any other university.

I have read and I understand the plagiarism provisions in the General Regulations of the University Calendar for the current year, found at `http://www.tcd.ie/calendar`.

I have also completed the Online Tutorial on avoiding plagiarism 'Ready Steady Write', located at `http://tcd-ie.libguides.com/plagiarism/ready-steady-write`.

Signed: ______________________ Date: ______________________

Permission to Lend and/or Copy

I, the undersigned, agree that Trinity College Library may lend or copy this thesis upon request.

Lokesh Selvakumar

August 19, 2022

A Solid-Powered Collaborative Rule Management Tool for Sharing Patient Data

Lokesh Selvakumar, Master of Science in Computer Science

University of Dublin, Trinity College, 2022

Supervisor: Dr David Lewis

The research of public mindset towards health information in Ireland revealed that there is a lack of awareness among patients concerning who has access to their health information. However, people believe that decisions involving access to their health information should be made in partnership with patients which forms the main motivation to carry out this research. The aim of the research is to transfer the power from the third parties to the patients who are the rightful owner of health information thereby offering a sense of data control to the patients. The research conducted proposes a Solid-powered collaborative rule management tool for sharing patient data which helps the targeted subjects (patient groups) to collaboratively agree on terms and conditions submitted by third parties in accessing their health information. This tool acts as an interaction medium between third parties and patient groups to collaborate and collectively decide the rules for accessing the patient data. Also, the same tool acts as a collaborative medium between patients to discuss and vote for the data access requests submitted by third parties. This research will benefit Patient groups where the individual data of the patients are stored in their Solid pods, which enables them to control who has access to their data and how their data is shared. Also, the Solid community will benefit from the collaborative rule management feature.

Acknowledgements

This MSc research project is very challenging and something out of my comfort zone for various reasons. I could not have accomplished it without the amazing support and guidance of so many different people.

I am grateful to Professor David Lewis for agreeing to supervise me in the development of this dissertation. I would like to thank him for his outstanding support and insightful ideas he has given me throughout the writing, research and development of this dissertation. I would like to thank my friend Beatriz Esteves, a PhD student from Universidad Politécnica de, Madrid,Spain belonging to Ontology Engineering Group for all the technical guidance provided by her which helped me a lot while working with Solid pods. Finally, I would like to thank my friends and family for all the support they have provided me in realising my goals.

Contents

List of Figures

List of Tables

1 Introduction

In this data-driven world, data corresponding to users who use applications and services are held by the company that provides them. This involves data involving both personal data like basic user information and sensitive data like educational records, employment records etc. This research seeks to transfer the power to control the individual data from third parties to its rightful owners thereby achieving a sense of data ownership. This research is focused on patient groups which is the target community for this research. It aims to provide a common collaborative medium for patient groups and third parties (healthcare professionals in public or private sectors like hospitals, community health, GP, social care, public servants in government departments and agencies like HIQA, HPRA, researchers) that wish to access the patient groups' medical data. The common collaborative medium is a software application built on top of a Solid pod which is used to decide the set of rules for accessing and processing the health data by involving both the patient groups and the third parties.

1.1 Motivation

The European Commission unveiled the European Strategy for new data spaces in February 2020, intending to develop a unified market for data sharing and interchange across industries that is both efficient and secure within the EU. The Commission's purpose is to advance the European data economy in a way that is consistent with European principles of self-determination, privacy, openness, security, and fair competition [2]. To achieve this, data access and use regulations must be fair, clear, and practical. For this research, we selected patient groups as our target subjects. The patients are always kept dark regarding their health information and its access to third parties. This is the main motivation behind this research, and I was motivated by the idea of data control this research offers to patient groups. The core idea of this research is to develop a collaborative tool that brings patient groups, healthcare professionals and third parties together to maintain, control and share medical data with third parties providing full control of medical data to the patient groups. The third parties must agree to these terms and conditions to access and use the medical data which transfers the power to control data from third parties to the rightful owners of data.

1.2 Research Question

The research question addressed by this research is as follows:

How to enable patient groups to collaborate to manage their own rules for sharing their personal health information with third parties?

This research question consists of the following three parts which form the key objectives of my research:

1. To develop a common medium for the third parties or companies that wish to access health data of patient groups to collaborate with the patient groups.
2. To develop features in the same common medium for the patient groups to collaborate among themselves.
3. To provision a safe, private storage space for the patients to store their health information.

1.3 Research Approach

Based on the above research Objectives, my research approach is as follows :

1. Surveying the state of the art in the patient data and Solid platform.
2. Understanding the existing rules for data sharing platforms.
3. Designing and implementing features involving collaborative rule development.
4. Evaluating the system developed in this research based on the use cases identified.

1.4 Contribution of Research

The final contribution of this research is a fully operational collaborative rule management tool which can be used to ensure that data of individual patients will be accessed based on rules agreed upon by both patients and third parties. By translating the goals to contributions, we expect to have the following contributions by the end of this research:

1. The tool facilitates mutual agreement between third parties and the patient group to access the health data. This tool helps the patient group to discuss among themselves the request submitted by the third parties.
2. The tool abstracts knowledge graph representation of rules while presenting the user-friendly readable structure of the rules encoded in the form of an open standard and extensible rule language.
3. Patients' concerns regarding health information sharing are addressed if they are using a platform like Solid which enables them to control their medical data sharing by imposing granular rules.
4. This study contributes to the web development community, the Semantic Web/Linked Data communities, and the Solid community. The Solid community may benefit from the collaborative rule management feature.
5. This research will help future Solid developers obtain actionable knowledge because there are only limited existing learning resources.

1.5 Report structure and contents

Related Work

This second chapter describes the research areas associated, Literature review strategy, health information and its landscape in Ireland, and State of the art of Solid. This chapter lays out all the background information needed to understand the research.

Solution and Design

This chapter describes the problem overview, identifies use cases, and solutions to the problem and then explains the design aspects involved in this research in detail.

Implementation

This is the fifth chapter of this document describing the technical architecture and technical implementation of the proposed tool.

Evaluation

This chapter deals with the evaluation of the tool developed as a part of this research. It starts by outlining the non-goals of this research and then discusses the security and privacy evaluation of the system. It is then followed by an evaluation of the tool in terms of goals achieved and scalability.

Conclusion and Future work

This section summarizes and concludes the whole research. It also includes future work that can be extended from this research.

2 Related Work

This chapter is split into three sections - the research areas associated with this research which gives an idea to the reader about the areas involved in this research, the current landscape of health information in Ireland which sets the context for the research, and finally the state of the art of Solid.

2.1 Research Areas associated

This project is an interaction of different research areas as shown in Fig. 2.1.

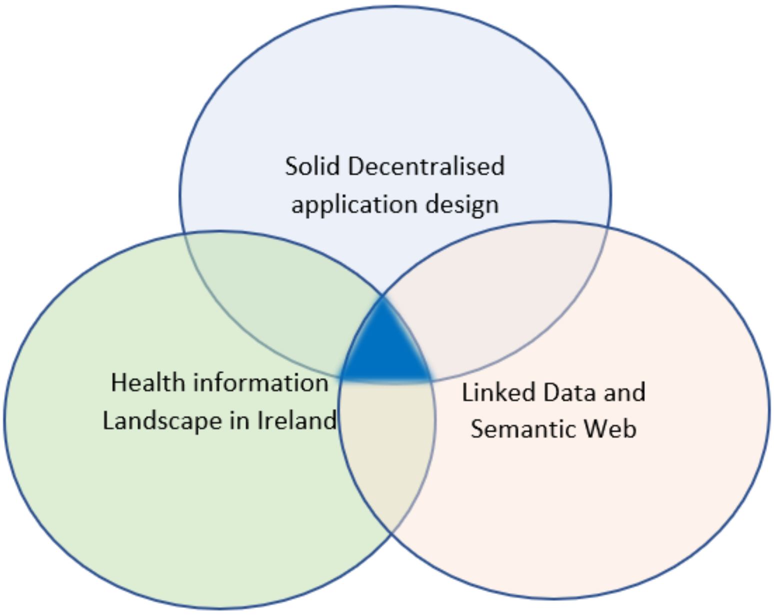

Solid Decentralised application design
Health information Landscape in Ireland
Linked Data and Semantic Web

Fig. 2.1: Research Areas

Solid pods
Solid linked data
Inrupt Javascript
Solid Identity provider
solid developer tutorial
getting started with Solid
Solid Tim Berners-Lee
Solid decentralised applications

Table 2.1: Literature review search terms for Solid

2.2 Literature Review Strategy

The literature review for this research is done by a technique called Snowballing [3]. A list of search terms was prepared by examining the concepts associated with Solid and the other research areas like health information landscape in Ireland, solid decentralised application design, linked data and semantic web. A list of articles was found by searching the already prepared list and then examining each article for relevant references. In addition to this, an ad-hoc search was also performed to add other references related to health information and its landscape. A considerable amount of blogs and articles from the web are also included due to the availability of inadequate resources as the Solid itself is new and growing. The word "Solid" is strongly associated with design principles involved in software engineering and this makes it difficult to use as a search term. This difficulty was solved by the snowballing technique used for the literature review as it was very effective where the relevant literature is found by association. The search terms used to identify Solid related articles can be seen in the table 2.1

IEEE Xplore[1], ResearchGate[2], Google Scholar[3], Inrupt Inc. web site[4], Web articles and blogs are the sources used to search for literature and any other relevant reference documents.

[1] https://ieeexplore.ieee.org/Xplore/home.jsp [Accessed: 17-08-2022]

[2] https://www.researchgate.net/ [Accessed: 07-08-2019]

[3] https://scholar.google.com/ [Accessed: 07-08-2019]

[4] https://docs.inrupt.com/ [Accessed: 17-08-2022]

2.3 Health Information and its Landscape in Ireland

2.3.1 Health Information

Personal information (also known as personal data) pertaining to a person's health status is referred to as health information. In addition to administrative and financial data about health (invoices for healthcare services, the scheduling of medical appointments etc.) this also contains medical data (such as medical examination reports, doctor referrals and prescriptions, radiography, laboratory tests, etc). Either the entire record or merely a portion of it may be referred to as "health information." Health information is regarded as sensitive information and is only permitted to be processed by medical experts who are obligated to maintain patient confidentiality.

Health information is described as per [4] as: "Health information is defined as information, recorded in any form, which is created or communicated by an organisation or individual relating to the past, present or future, physical or mental health or social care of an individual or group of individuals (also referred to as a cohort). Health information also includes information relating to the management of the health and social care system."

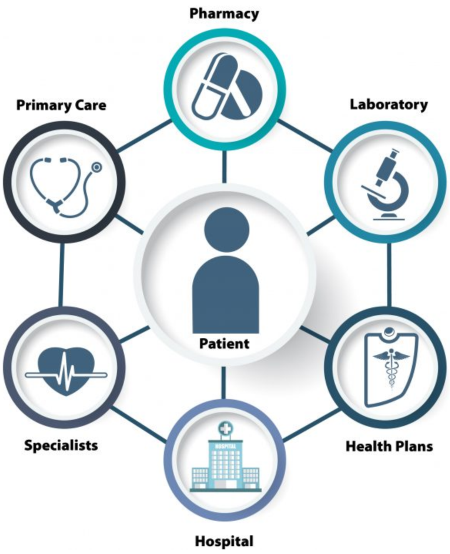


Fig. 2.2: Patient health information [1]

2.3.2 The infrastructure of health data in Ireland

An overview of the healthcare system in Ireland is given to lay the context for this research. The important measures in health information systems that were implemented in historical order as the ESRI survey and statistical report [5]:

- The Health Act of 2007[6]: This saw the creation of the independent Health Information and Quality Authority (HIQA), which is responsible for setting data and information standards for Irish health and social care services. When it comes to different aspects of HIS and eHealth in Ireland, HIQA has offered vital expert insight. It also actively participated in educating policymakers during COVID-19. In addition, HIQA plays a significant role in disseminating knowledge about IHIs and HIS.

- Health Strategy for Ireland 2013: This measure outlined how to introduce and use eHealth and health data appropriately and effectively in Ireland. A new organization called eHealth Ireland, which is a part of the Health Service Executive (HSE), was given a new organizational responsibility. In addition to collaborating with academic and business colleagues on many eHealth initiatives, eHealth Ireland is at the forefront of the creation of numerous initiatives in the health service. Services and support for Information and Communication Technology (ICT) are provided by the Office of the Chief Information Officer (CIO) to the HSE.

- Health Identifiers Act of 2014: This Act established the Individual Health Identifier as a new type of legal entity (IHI). It lays the groundwork for the National Register of Individual Health Identifiers and the National Register of Health Services Provider Identifiers to be established legally.

- Knowledge and Information Strategy: providing the benefits of eHealth in Ireland 2015 – this measure was built on the previous 2013 eHealth strategy, which described how integrating information and enabling technology will assist the delivery of innovative healthcare inside the Irish healthcare system.

- National Electronic Health Record: Strategic Business Case 2016 – this publication provided a Strategic Business Case for the investment of up to €875 million to implement a national Electronic Health Record (EHR) throughout the Irish healthcare system.

- The 2018 PA Consulting Capacity Review: This offered information on the capacity needs for the health and social care system. It emphasized the need to invest in Information and Communication Technology (ICT) infrastructure, specifically, eHealth: eHealth and Information and Communication Technology (ICT) were universally considered important enablers to establishing a more effective and integrated health system. Improved data gathering would also help with planning for population health needs.

- The Sláintecare Initiative 2018: The ten-year Sláintecare program aims to modernize social and health care in Ireland. It plans to change Ireland's healthcare system from a two-tiered to a system based on medical needs. The Irish Department of Health asked the European Union for technical assistance in creating a framework for the health system performance assessment (HSPA) in order to support the implementation of the Sláintecare [7]. On the "Performance accountability for the Irish health system" project, an outside research team was hired to collaborate closely with the Irish health authorities.

The current infrastructure in Ireland's health and social care sector is severely fragmented, with significant gaps and information silos that prevent the safe, effective movement of information, despite the fact that there are several examples of exemplary practice. As a result, individuals who use services are repeatedly prompted for the same information. The Irish health system's data infrastructure and Health Information Systems(HIS) both have severe shortcomings. Even though the creation of eHealth Ireland has resulted in numerous achievements, significant investment is still needed. Similar to prior years and less than peer nations, which spend up to 3% of their healthcare budget on health technologies, Ireland spends less than 0.8% of the public health budget on eHealth and other health technologies in 2021 [5]. The COVID-19 pandemic brought to light the nation's health information system's limitations as well as its potential for quick growth and development. The evaluation of the HIS in Ireland [7] aided in the creation of a national Health System Performance Assessment (HSPA) framework and sparked efforts to improve data governance and infrastructure as well as move the country closer to a person-centered, data-driven health care system.

2.3.3 Third parties involved in health data

Understanding the involvement of these parties is essential to fully protect the rights and privacy of the patients regarding their health information. The following are the important third parties referenced from the report[8] involved in accessing, storing, and using the health information for various purposes:

- Healthcare professionals in the private or public sectors like hospitals, General practitioners, social care, and community health who are seeking access to health information for improving services to patients, change and innovation. They also act as a creator of health information.

- Public servants in government agencies and departments like HIQA, and HPRA who are seeking access to health information for the legislative policy or practice change.

- Academic or clinical researchers who are seeking access to health information to complete health research which is publicly or commercially sponsored.
- Professionals from private health firms accessing health information for the purpose of conducting research or creating new medical innovations (medicine, device, vaccine).

2.3.4 Usage of health information

Direct individual care can be provided using health information, and it can also be utilized for other things like service planning and research. The utilisation of a person's health information for their own diagnosis, care, and treatment by health and social care experts is referred to as "individual care." Information used for direct care is frequently referred to as the primary use of health information. The use of a person's health information for purposes other than their own diagnosis, care, and treatment is referred to as "secondary use of information." Service planning and research are the two main categories of secondary usage. Also sometimes health information will be altered making it difficult or impossible to identify the real person from whom the data was taken in order to safeguard that person's privacy.

2.3.5 Health Information and Quality Authority (HIQA)

To advance safety and quality in the delivery of health and social care services for the benefit of the general public's health and welfare, the independent statutory organization known as the Health Information and Quality Authority (HIQA) was created. The scope of HIQA's mandate currently encompasses numerous services provided by the public, corporate, and nonprofit sectors. HIQA is accountable for the following under the direction of the Minister of Health and in collaboration with the Minister of Children and Youth Affairs:

- Setting standards for health and social care services
- Regulating health services
- Regulating social care services
- Health technology assessment
- Monitoring services
- National Care Experience Programme
- Health information

2.3.6 Consent in the context of processing health information

The two types of consent [9] are Opt-out (implied consent) and opt-in (explicit consent):

- Implied consent – Unless a person expressly objects, data will be automatically gathered and utilized with the assumption that consent has been given.
- Explicit consent – a person actively agrees or opts in to permit the collection or use of their data.

However, the GDPR clearly makes the implied consent unacceptable and as it must always be given through an opt-in, an active motion or a declaration so that there is no misunderstanding that the data subject has consented to the particular processing [10].

The General Data Protection Regulation (GDPR) defines consent [11] as: *'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*

2.3.7 Legislation related to data protection

Data Protection Acts (1988–2018)

The gathering and processing of personal data are governed by these Data Protection Acts. In 1988, the Data Protection Act was enacted. In order to implement the EU General Data Protection Regulation 2018 (GDPR, 2016/679), it was once more revised in 2018. It created a new Data Protection Commission to serve as the entity responsible for overseeing and enforcing the data protection requirements set forth in the regulation and directive. The Legislation Enforcement Directive (Directive 2016/680/EU) is also incorporated into national law by the Act. In 2018, the Department of Health unveiled the Health Research Regulations. Additionally, they plan to create two more sets of guidelines for the use of health data in planning services and for personalized treatment. The Health Research Regulations 2018 give further and more precise effect to the adequate and specific procedures for data processing stipulated in Section 36 of the Data Protection Act of 2018.

The Health Research Regulations 2018

The Health Research Regulations 2018 [12]:

1. outline the mandatory suitable and specific measures for the processing of personal data for the purposes of health research (Regulation 3(1))

2. provides a definition of health research for the purposes of the regulation (Regulation 3(2))
3. provides for the possibility of applying for a consent declaration for new research (Regulation 5)
4. provides for transitional arrangements in respect of the granting of consent declarations for health research that is already underway (Regulation 6)
5. provides for the establishment and operation of a committee of persons to make decisions on applications for consent declarations, including an appeals process (Regulation 7-13 and Schedule)
6. includes a number of miscellaneous provisions (Regulations 14-16)

The General Data Protection Regulation (GDPR) 2018

A framework known as the General Data Protection Regulation(GDPR) [13] came into effect across the European Union on 25 May 2018. An accompanying Directive known as the Law Enforcement Directive establishes data protection standards in the area of criminal offences and penalties. Both the General Data Protection Regulation(GDPR) and the Law Enforcement Directive cause significant reforms to existing data protection rules. They put extra requirements on organizations that process personal data and set tougher standards for individual data protection. They also broaden the range of penalties that could be imposed when these rules are broken. Article 9 of the GDPR addresses the processing of special categories of personal data, such as health data.

2.3.8 Surveys and their findings

The Irish Platform for Patient Organisations, Science and Industry(IPPOSI) is a patient-led organisation that places patients at the heart of health policy and innovation. IPPOSI works with government, patients, industry, science and academia. To explore who should have access to health information, for what reasons (beyond direct treatment), and with what protections are in place, IPPOSI invited 25 people representing a cross-section of Irish society to participate in a Citizens' Jury on Access to Health Information in April 2021 [8]. After three weeks of long and careful discussions, the jurors concluded that methods, processes, and policies designed to manage or distribute health information must be made in conjunction with patients and patients must own their health data. The IPPOSI further wanted to understand the public and patient attitudes towards access to health information. Therefore, they conducted two surveys [14], the first survey involving the patient organisation leaders and the second survey involving patient organisation members. The survey results concluded that the patients have almost little to no knowledge about health information gathered about them and how they are shared.

The National Public Engagement on Health Information was conducted by three organizations namely the Health Information and Quality Authority (HIQA), the Department of Health and the HSE between 2020 and 2021 [15]. The three organizations joined together to conduct this engagement program with the aim of understanding the Irish public related to the collection, sharing and use of personal health information. This National Public Engagement survey involved public members of over 1200. The telephonic survey involving people over 1220 and engagement with focus groups involving 14 groups(85 people) were the two survey methodologies used. The findings in terms of the use of health information for direct patient care show that 97% of the people feel that it is important that a hospital doctor has access to accurate health information, while 90 % of the people trust General Practitioners(GPs) to keep their information safe and secure in addition to sharing only relevant information. However, 71 % of the people would like to know what information is shared between GP and hospital. The findings in terms of the use of health information for purposes beyond direct patient care reveal that 94 % of people think that it is important that health information is used to improve the quality of care provided to patients. Also, 93 % of the people involved in the survey think it is important that health information is used to plan healthcare services. However, 77 % wanted to know how their health information is used beyond direct care. Almost all the people involved in the survey agreed that doctors can access their digital records and also can access electronic health information when they are unconscious without their permission, however, 82 % of people feel that it is important to know which healthcare professionals view their digital record.

2.3.9 Summary

To summarize, Ireland is seeing major improvements and movement toward digital records for health information and there are no standard practices in sharing information with third parties. As an initial step to understanding the current landscape of health information in Ireland and also to find any existing solution to the problem addressed in this dissertation, the relevant literature review is done. Healthcare professionals (hospitals, GP, community health, and social care) capture patients' medical information and it will be stored, and maintained on their own infrastructure. The two major pieces of legislation that allow patients to view their medical data are the Freedom of Information Act of 2014 [16] and the Data Protection Act of 2018 [17]. The 2018 Data Protection Act was subsequently incorporated into the General Data Protection Regulation. Though there are multiple legislation and laws available, General Data Protection Regulation (GDPR) is the law that mandated explicit consent in processing the information.

Though patients have the right to access their medical information by requesting access from healthcare professionals, this information is not controlled or maintained by the patient. It is not an easy process to access their health information and often people feel that they are unaware of who has access to their health information. Often the people are repeatedly asked for the same information thus making the data redundant which clearly indicates that there are no standard practices that exist in reusing the same information. People in Ireland are supportive of the use of electronic records, according to a recent national public engagement on the subject, but they want more information about how their privacy is safeguarded and when and how their information is shared. As a result, this study is a small initial step toward closing all of the previously mentioned gaps in health information and patient care.

2.4 State of the art of Solid

2.4.1 Semantic web and Linked Data

The Semantic Web (SW) is not a Web that is separate from the current one but it is an extension of the current Web in which information is given well-defined meaning and relationships between data, rather than just documents, are defined in a common machine-readable format resulting in a Web of Data [18].

Linked Data is simply the process of using the Web to create typed links between data from various sources. Technically, Linked Data is data published on the Web in such a way that it is machine-readable, its meaning is explicit, it is linked to other external data sets, and can be linked to from other external data sets [19]. Linked Data is nothing more than a set of best practices for publishing data and Solid relies on Linked Data principles [20]. The idea is to create and implement standards for linking published structured data that freshly created data can discover and link to. A crucial part of the linked data movement is the discovery of new data sources. Although not all data is created in the same location, web standards can aid in the development of the Semantic Web. Currently, Linked Data is based on two technologies namely Resource Description Framework (RDF)[5], and Hypertext Transfer

[5] https://www.w3.org/TR/2014/NOTE-rdf11-primer-20140624/ [Accessed: 18-08-2022]

Protocol (HTTP)[6].

A brief description of the Ontology and Knowledge graph is given below to understand the context of Solid.

The word **"Ontology"** refers to the formal naming and definition of the properties, types, and interrelationships of the entities (types) for a specific domain of discourse also known as the domain model. For example, health domain, finances, telecommunications, etc.

Knowledge Graph is a combination of technologies, specifications, and data cultures for densely interconnecting (Web-scale) data across domains in a human and machine-readable and reasonable way. The term knowledge graph itself does not prescribe any particular technology stack. More formally, a knowledge graph (as a set of statements) can be thought of as a node and edge labelled directed multigraph. The largest publicly available knowledge graph is the so-called Linked Data cloud based on the RDF/Semantic Web technology stack [21].

2.4.2 Solid

Solid is a web decentralization project led by Sir Tim Berners-Lee, the inventor of the World Wide Web, developed collaboratively at the Massachusetts Institute of Technology. Solid is a specification aimed to achieve true data ownership and improve privacy. Solid is based on Linked Data [22]. Solid, like any other standard, only specifies the interaction model with which the system must comply.

Building blocks of Solid

The following are the basic building blocks of the Solid platform:

1. **Pods:** Pods are decentralised personal online web data servers that let people securely store their data. Pods can be used to store all kinds of data from structured data to regular files that people store in a Google drive or dropbox folder. Through pods, people can grant and revoke access to any slice of their data stored in the pod. There are two ways a user can get a pod - by hosting their own pod or signing up with any existing Pod provider to use their Pod services. Pods are provided by multiple Pod providers and each Pod provider is free to use any underlying technologies for their Pod implementation. As with most Web-based systems, the Pod provider merely provides a REST read-write interface to the clients, with storage technology being unimportant to the users. Each Pod provider has its own way of interacting with the storage. The

[6] `https://www.rfc-editor.org/rfc/rfc7230` [Accessed: 18-08-2022]

Pod provider might have data stored without encryption, but it must be Solid complaint (resources in folders). A user or patient can store their data in one or more Pods and programs can read and write data into the Pod based on the permissions allowed by the user or users associated with that Pod.

2. **WebID:** WebID is an Internationalised Resource Identifier (IRI) which is unique, and it can be dereferenced as a FOAF profile document serialized in RDF [23]. WebID-OIDC protocol which adds a layer on top of the OpenID Connect protocol which in turn is built on top of the OAuth 2.0 protocol is used to authenticate and authorize users or organizations to access the Pods. To share data with a third party, a user links their sharing choices to that third party's WebID.

   An example of a WebID:`https://lokesh.inrupt.net/profile/card#me`

3. **Resource Description Framework (RDF):** Using the Resource Description Framework (RDF), one may express information about resources [24]. Resources can be documents, living beings, tangible things, conceptual ideas and can be anything. RDF is designed for scenarios where web content needs to be processed by applications rather than only displayed to users. RDF offers a standard structure for representing this data so that it may be exchanged between applications without losing any of its original meaning. RDF can be used, for instance, to publish and link data on the Web. RDF [24] is a W3C Recommendation that expresses factual information in triples. An RDF triple is a combination of subject, predicate and Object.

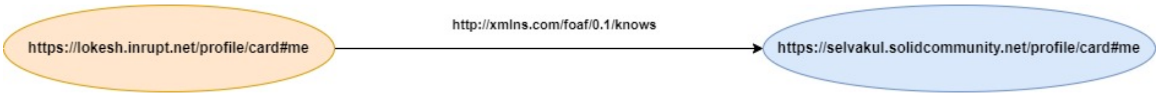

https://lokesh.inrupt.net/profile/card#me
http://xmlns.com/foaf/0.1/knows
https://selvakul.solidcommunity.net/profile/card#me

Fig. 2.3: Graphical representation of RDF triple

   An example of an RDF triple is represented in the Fig.2.3. It is equivalent to the English sentence "The person represented by WedID https://lokesh.inrupt.net/profile/card#me knows the person with WebID https://selvakul.solidcommunity.net/profile/card#me".

   In the example represented by Fig.2.3,
   https://lokesh.inrupt.net/profile/card#me is the *Subject*,
   the FOAF [25] vocabulary **http://xmlns.com/foaf/0.1/knows** is the *Predicate*,
   the WebID **https://selvakul.solidcommunity.net/profile/card#me** is the *Object*.

4. **Hypertext Transfer Protocol (HTTP) RESTful API:** Solid offers a RESTful API, expanding the LDP principles, while LDP specifies a framework for HTTP-based com-

munication with Linked Data Resources [7]. Depending on access restrictions, any Solid application that communicates with the Pod could use this API to carry out Create Read Update Delete (CRUD) operations on resources and Containers. For publish/subscribe apps, there is also a WebSockets API accessible in addition to this REST API.

5. **Web Access Control (WAC) [26]:** The WAC protocol specifies how to make it possible for applications to identify authorizations tied to a certain resource and to manage these rules. The server oversees the relationship between a resource and an Access Control List (ACL) resource and applies the permission requirements to operations that are requested. In order to express and ascertain the access privileges of a requested resource, authorizations are expressed using the ACL ontology. According to the ACL ontology, any type of the following access can be granted to a resource. This specification makes use of the read, write, append, and control resource operations classes as well as other access modes currently specified by the ACL ontology. An authorization might impose the necessity for authenticated agents or grant public access to resources. Agents and resources might come from several origins.

6. **Linked Data Notifications (LDN):** At its most fundamental level, Linked Data Notifications [27], or LDN, is a protocol for push message communication and a W3C recommendation. Users can only communicate via Solid in this fashion because it is the only way that has been specified for Pods to do so. The sender and receiver agree on a shared area on the recipient's Pod where the sender can only produce resources (messages), and the recipient can respond to those messages at a later time. Similar to a straightforward mailbox, the sender only has access to Append while the receiver who is the owner of the Pod has full access. Inbox is the name of the receiver's endpoint according to the LDN Specification.

How does Solid relate to other Web standards?

Solid is based on web standards that are already in place. Pods and apps can still be accessed with the same browser on the same computer. Instead of signing into Google and Facebook, the users or patients can sign in with Solid provider and won't be tracked. The patients or users get to choose which app to use and which pod to use with which app. The application stores all the data on Pods and no data is stored on the application itself. LDP and WAC (WAC draft), both based on HTTP and RDF vocabularies, are used in the core Solid specification. Solid uses WebID-TLS and/or OIDC for identification.

[7] `https://www.w3.org/TR/2015/REC-ldp-20150226/#specs-http`

3 Solution and Design

This chapter gives an overview of the problem that is being addressed in this research and outlines the use cases identified from the problem. It also provides detail about the design of the project involving functional requirements, functional architecture, and design choices.

3.1 Problem overview

As discussed in the previous chapter, the landscape of health information in Ireland is very scattered and not centralised. Post pandemic, most of the time the patients have to give the same information multiple times leading to more confusion and data discrepancies. In addition to that, individuals or patients have little to almost no knowledge of who owns and has access to their health information. And there is a significant amount of interest among individuals to own their health information and manage who has access to it [8]. Based on the above information, there are major gaps in health information management and how it is shared. So the research question that is framed based on surveying the state of the art in health information is how to help patient groups create rules for sharing their personal health information with third parties in collaboration with the healthcare professionals and third parties that wishes to access them.

3.2 Use cases

Based on the problem overview 3.1, the following general use cases were identified. Patients belonging to patient groups, representatives of the patient groups and third parties are the three actors identified that are external to the system boundary.

use case 1

Patient groups also need a collaborative medium for themselves to discuss among them the data access request submitted to them by third parties for accessing the health information.

use case 2

Patient groups and third parties need a common medium to collaborate and agree to the terms and conditions for using the medical information of the patients.

use case 3

Patients need a secure private space or storage system to store their health information created by health professionals.

3.3 Solution proposed

There are multiple ways to solve the problem addressed in this research. However, all the solutions have to revolve around the idea of bringing together patient groups, third parties and health care professionals to collaborate with each other agreeing to a common framework of rules in managing health information. A Naive approach to solve this problem would be arranging a meeting in person to draft rules that will be used in accessing the health information of patients. The drawback of this approach would be frequent meetings which are practically very inefficient as it consumes more time for all the parties involved. More time and more resources will be spent on organizing meetings and finding a common time frame that suits all the parties involved rather than solving the problem itself.

Since this research is carried out in the field of computer science and having a good practical background in software engineering involving a considerable amount of experience in developing software applications, I propose a software application where all the parties involved in the health information can come together and collaborate in a transparent way to agree on rules for using the health information of the patient groups. This eliminates the need for in-person meetings and anyone can access it in their own leisure time thereby making the whole process seemingly fast and efficient. There are numerous ways to build a software application. The application can be built using the most popular technologies available in the market like React, Flutter, and Angular for building the user interfaces and spring boot, node.js, and Django for the backend servers. There is a number of options available for the databases like

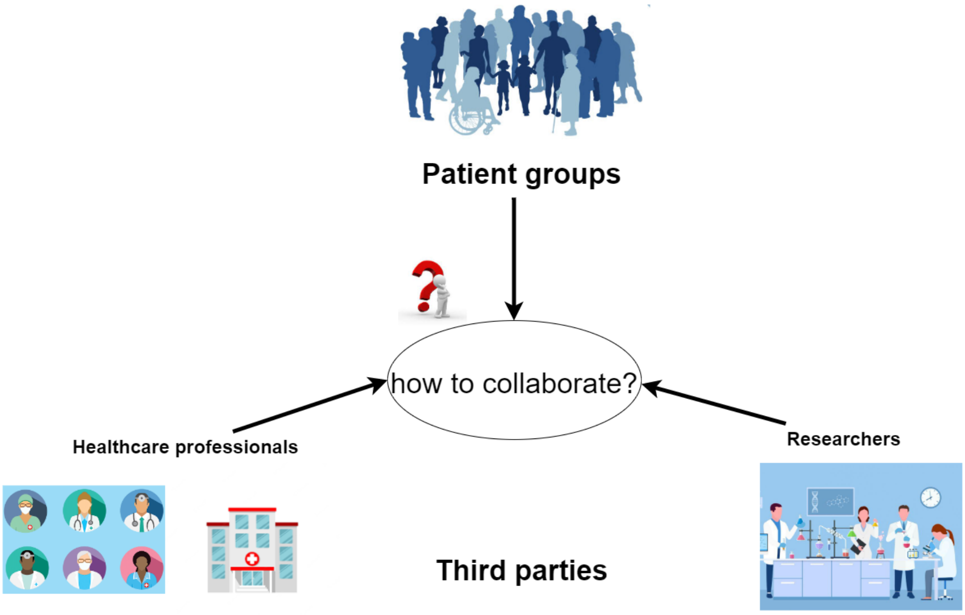


Fig. 3.1: Research problem

MySQL, Postgres, Firebase, etc. However, this research presents a unique way of developing the software by making use of Solid, an initiative from the father Of The World Wide Web, Tim Berners-Lee. By making use of Pods and Solid, the whole system moves under the Solid ecosystem thereby eliminating any need for the above-mentioned databases. The data is not bound to the application and Solid helps us to create a decentralised application. The data stored and accessed in Pods uses standard interoperable protocols and data formats.

3.4 Functional Requirements

Based on the Fig.3.3 which depicts the use cases considering the system boundary, the following functional requirements are identified.

Functional Requirement 1 - Sign Up with Pod Provider
The software tool developed should allow users (patients and third parties) to select a list of well-known public Pod Providers to sign up for the collaborative tool with pod providers.

Functional Requirement 2 - Log In with Pod Provider
The collaborative tool should allow users (patients, third parties and representatives) to select a list of well-known public Pod providers to log in using WebID authentication in the Pod providers thereby enabling them to log in for the collaborative tool with pod providers.

Functional Requirement 3 - Create and Submit Data Access Request

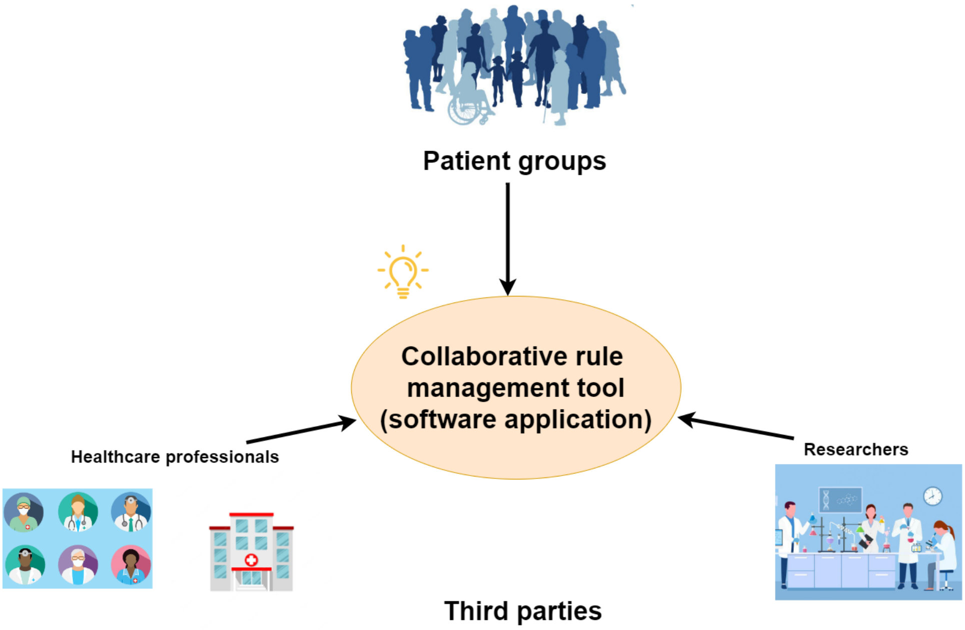


Fig. 3.2: The solution to the problem

The proposed application should allow the third parties who wish to access the patient groups' health information to create and submit data access requests to the patient groups.

Functional Requirement 4 - Review Data Access Request submitted and take action

The proposed application should allow the third parties to review the data access request submitted and act on the requests sent back from the patient groups. They should be able to accept or reject the request submitted back by the patient groups.

Functional Requirement 5 - View Data Access Request submitted by third parties and collaborate

The proposed tool should allow patient groups to view the data access request submitted by the third parties. The patients should have features to upvote, downvote and comment on each rule in the request. This helps them to collaborate among the patient groups.

Functional Requirement 6 - Representative review patient discussions and take action

The collaborative tool developed should have features enabling the representative or administrator of the patient groups to review the patient discussions. This can help him to take a decision on whether to accept or reject the request. Features like editing and submitting back the request to third parties should also be available.

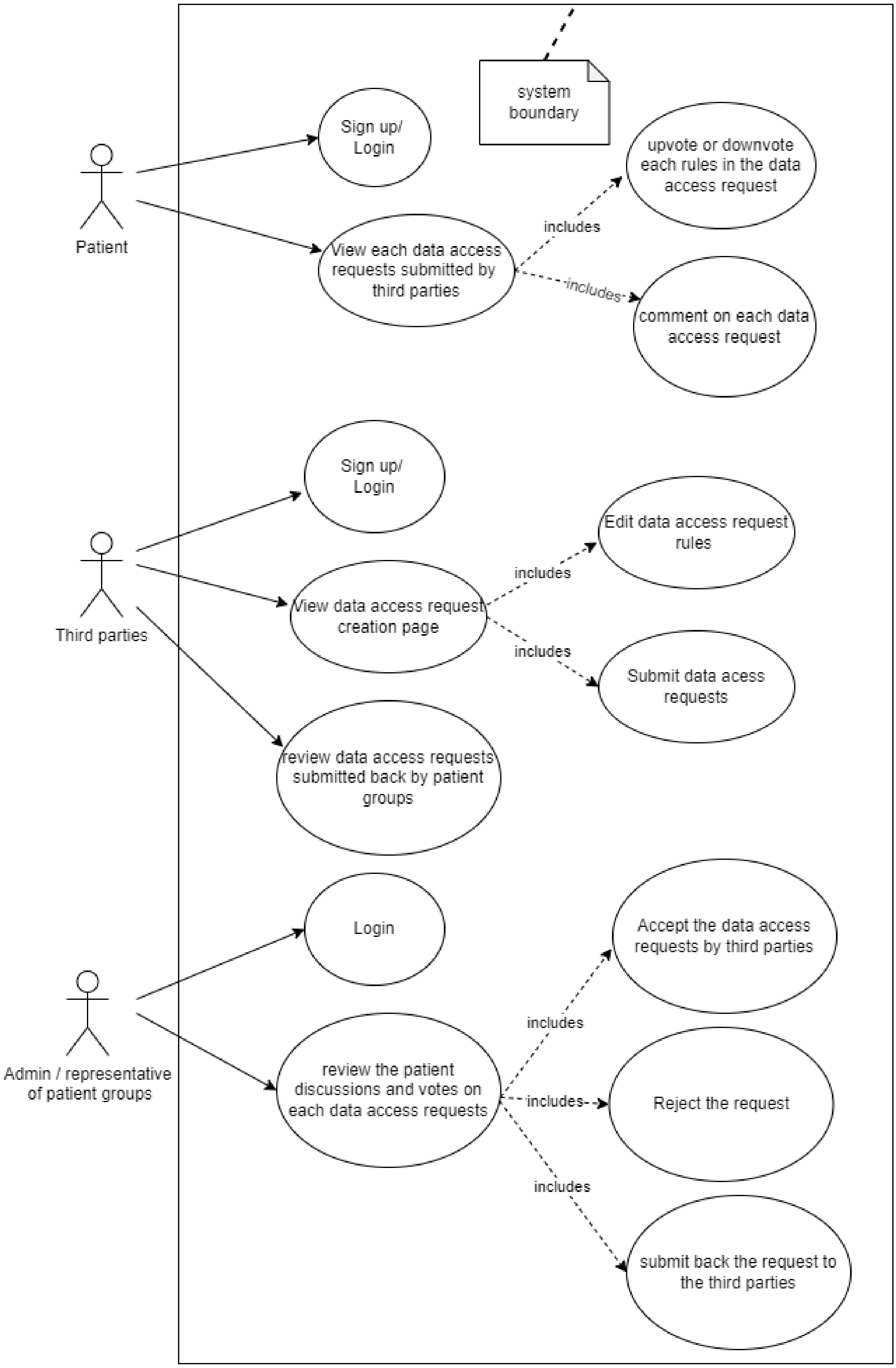

system boundary
Patient
Sign up/ Login
View each data access requests submitted by third parties
includes
upvote or downvote each rules in the data access request
includes
comment on each data access request
Third parties
Sign up/ Login
View data access request creation page
includes
Edit data access request rules
includes
Submit data acess requests
review data access requests submitted back by patient groups
Admin / representative of patient groups
Login
review the patient discussions and votes on each data access requests
includes
Accept the data access requests by third parties
includes
Reject the request
includes
submit back the request to the third parties

Fig. 3.3: UML diagram for use cases

3.5 Functional Architecture

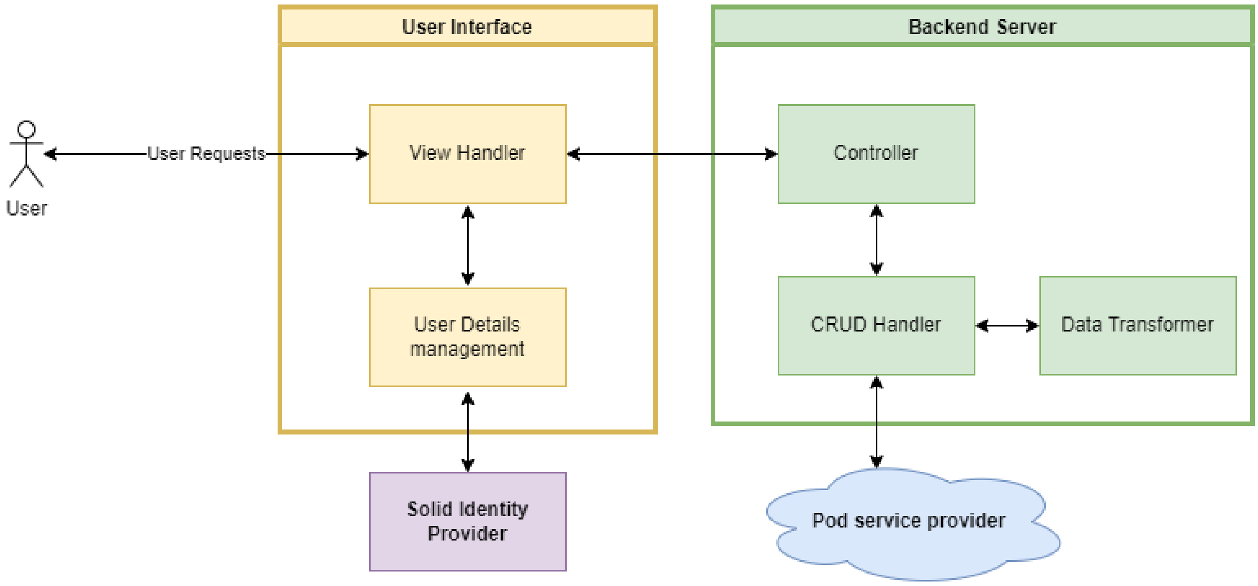


Fig. 3.4: Functional Architecture

The Fig.3.4 shows the functional architecture which reveals the components clustered together according to their functionality.

1. **View Handler**: This component is responsible for deciding the pages to be displayed. It takes user requests as its input and renders corresponding views back to the user. The user interacts with the View Handler. View Handler interacts with the User Details Management component to identify users and also with the Controller in the node server to submit user requests.

2. **User Details Management** User Details Management component is responsible to identify the existing users and sign up the new users by connecting with the Solid identity provider.

3. **Solid Identity Provider** Solid Identity Provider provides the option for any user to sign up and own a solid pod thereby providing a unique WebId to each user to identify them.

4. **Controller** The controller is a server component that handles all the incoming requests from the user interface through client interaction. The HTTP requests are mapped to corresponding REST API endpoints.

5. **CRUD Handler** This component is responsible for performing Create, Delete, Update

and Delete (CRUD) operations in Solid pods. This acts as an intermediary between Solid pods and Controllers. This is connected with Controller, Data Transformer and also pod service provider.

6. **Data Transformer** The CRUD Handler makes use of this component to transform the data access request parameters to ODRL policy. Data Transformer is responsible for the conversion of all the data involved in the application to knowledge graph representation that can be stored in the pods.

7. **Pod service Provider** A cloud pod service provider through which a pod server can be created and used. In the proposed application, two Pods will be used. One is supposed to hold patient groups' medical information and the other Pod belongs to the third-party user who submits the data access request.

3.6 Why Solid Pods?

All the technical details and building blocks of the Solid are mentioned in the section 2.4. Solid and Pods are used in this research and it forms the backbone of this research. No other conventional databases (relational database, NoSQL database etc) are used because of the following reasons.

- Solid uses decentralized data stores called Pods.
- User can have their own personal Solid Pods where they can store any information.
- User can grant access and revoke access to any of the resources in his Pod.
- The information is not bound with any application.
- The information stored can be made machine-readable and represented in Knowledge graphs.
- Solid supports all the file storage formats a Google drive or dropbox supports.
- It is a movement towards the Semantic Web.
- Solid promotes true data ownership and improves privacy.

In this project, the usage of Solid Pod is an elegant choice as the ultimate goal in this research is the transfer power to patient groups to actively control their own medical information by involving them to manage their own medical data collaboratively. However, this is not possible with any other databases as it can be application-specific and not user-specific.

Even if such a use case should be realised with other databases, it involves building another application to actively change data. Solid and its ecosystem is fully designed with the idea of each individual controlling their own data and they can easily migrate their data to any other application because the data is not bound with any application.

3.7 Framing Data access request rules

If an organization or third party is using a person's personal information, then the corresponding person is called the data subject. The third-party holding the information or using the information is known as a data controller. The data controller can allow another entity or another person to process this information. This entity or a person processing the data is known as a data processor [28].

Based on GDPR guidelines regarding accessing personal data, if personal data is processed or being stored, then the person whose personal data is processed or stored has the right to know [28]:

- The reason for which it is being processed
- with who the personal data will be shared with
- How long the personal data will be accessed or kept

To prototype the functionality of creating Data access requests in the software tool, the following set of template rules are framed taking the above points into consideration:

1. Patient data access till <date> (a <date> selection feature)
2. Patient data will be used for the following purposes: Research, Analysis (check box to select list of purposes)
3. Patient data will be sold to the third parties (yes/no dropdown menu selection)
4. history of patient data will be maintained (yes/no dropdown menu selection)
5. patient data will be copied (yes/no dropdown menu selection)

3.8 Why Open Digital Rights Language (ODRL) for rules?

Solid pods rely on very simple access permissions using Access Control Language (ACL) expressions. Personal online datastores (Pods) from Solid are ideal for storing personal information because they allow users to represent access permissions in a very simple way using Access Control Language (ACL) expressions. While these expressions are adequate for yes/no and read/write permissions, they are incapable of representing more complex rules or invoking regulatory-specific concepts. Therefore this research makes use of an extension of the ACL language and algorithm to implement consent and data requests referenced from the previous work [29]. The rules are stored as the Open Digital Rights Language (ODRL) policy, which permits the expression of complex rules, and the Data Privacy Vocabulary (DPV), which allows for the use of privacy and data protection terms.

4 Implementation

This chapter discusses how the design proposed in the previous chapter was implemented to build a collaborative rule management tool(CRMT) for sharing patient data. It starts with an overview and then the section 4.1gives a detailed description of the technical architecture of the proposed tool and the section 4.2discusses in detail the alternative frameworks considered for each layer in the technical architecture. Finally, this chapter ends with the technical implementation section describing the developed tool and its features.

4.1 Technical architecture

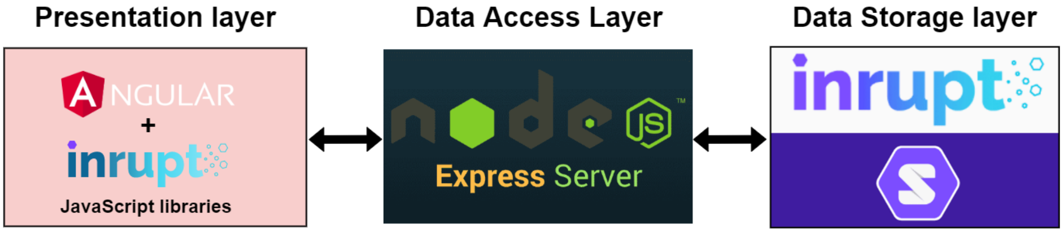


Fig. 4.1: Technical Architecture

This is a web application targeted for web browsers and not for any other platforms. This is due to the fact that the resources and libraries for Solid related development are available only for web application development. The technical architecture of the patient health data collaborative rule management tool as shown in Fig.4.1 has three layers namely the presentation layer, backend server layer and Inrupt Solid pod layer.

1. **Presentation Layer:**This layer is responsible for the user interaction. The tool proposed in this research is a web application created using the Angular framework (version 14.0.0) along with Inrupt's JavaScript libraries. The Inrupt's JavaScript libraries used are @inrupt/solid-client, @inrupt/solid-client-authn-browser, @inrupt/solid-client-authn-node and @inrupt/solid-client-access-grants.

2. **Data Access Layer:** This is the intermediate layer between the data storage layer and the presentation layer. It is a backend server built using Node.js with the express framework. This is responsible for handling user requests from the presentation layer, verifying login credentials and signup requests, and the CRUD(Create, Read, Update and Delete) operations.

3. **Data Storage Layer:**This acts as a data storage layer that holds user information necessary to use the application and data generated using the application. This layer is made up of a solid pod provided by Inrupt.net. As far as the proposed application is concerned, this layer is the combination of Solid Pod of patient groups that holds all the patient groups' data and the third party's Solid Pod that creates the data access request.

4.2 Alternatives considered

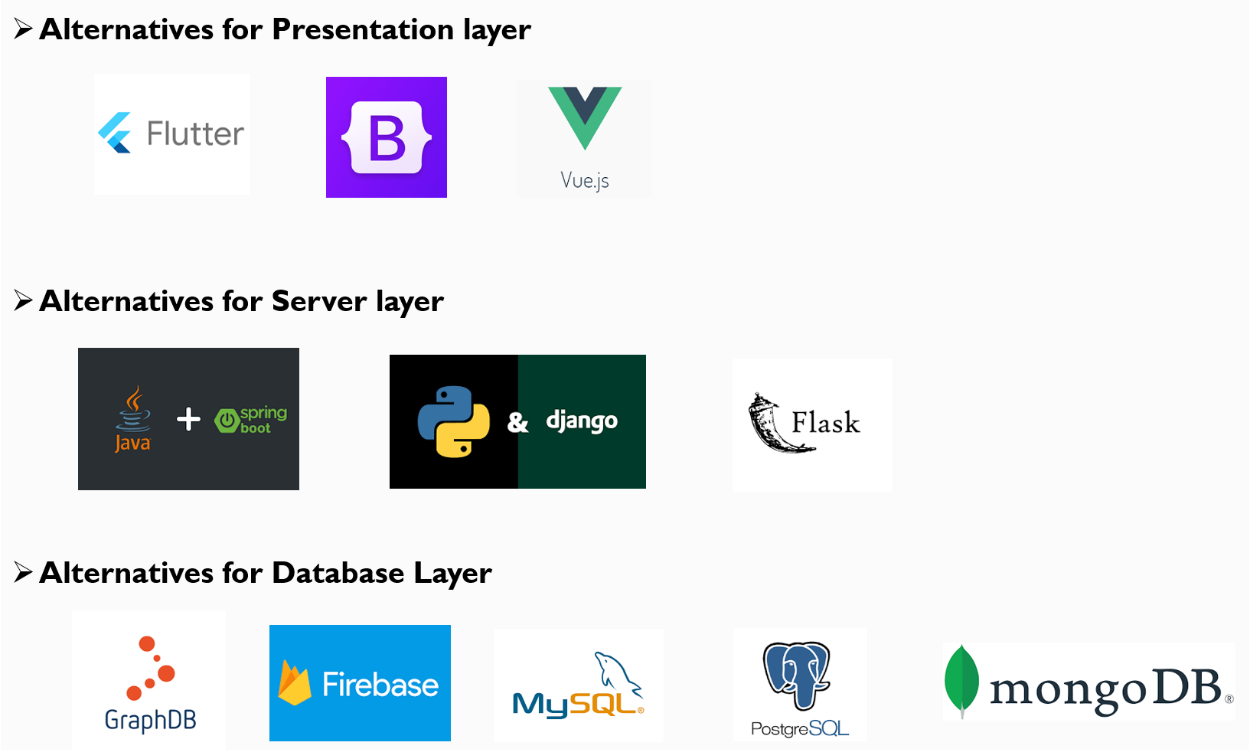

➤ Alternatives for Presentation layer
Flutter
B
Vue.js
➤ Alternatives for Server layer
Java
+
spring boot
&
django
Flask
➤ Alternatives for Database Layer
GraphDB
Firebase
MySQL
PostgreSQL
mongoDB

Fig. 4.2: Alternatives considered for each layer

Flutter, Bootstrap and Vue.js are the alternative frameworks considered for building the User Interface of the tool. Flutter has got a good community backed up by Google which supports a single code base to develop software for multiple platforms like mobile, web etc.

However, Flutter does not have any support to add external Inrupt JavaScript libraries. Bootstrap is a great option but it does not come with an inbuilt server and packaging tool. Vue.js is an excellent front-end framework, however, the lack of expertise in using this framework made it impossible to implement in this project. So, Angular is chosen as the front-end framework which helped me to seamlessly integrate Inrupt JavaScript libraries to work with Solid Identity provider and Pod-related functionalities.

The most popular existing server layer frameworks for developing RESTful endpoints are spring (Java), Django (python) and Flask (python). Spring does not support Inrupt JavaScript libraries which is essential because the server layer should be interacting with the Inrupt Pod services. Python has some libraries to interact with Pod however I have no prior expertise in using them. Since Node.js is purely based on JavaScript, it is easy to code and front-end developers can code easily without learning new programming languages for programming the server layer. Also, Node.js with Express.js provides excellent features to develop RESTful endpoints. Since library packages of Inrupt JavaScript are published in npm libraries, it provides easy integration with Inrupt Javascript libraries.

4.3 Technical Implementation

4.3.1 Development Environment

The following are the details of the development environment used to create the Solid-powered collaborative management tool for this research:

1. **Operating System:** Windows 10 Home Single Language 64-bit operating system, X-64 based processor
2. **Integrated Development Environment (IDE):** Visual Studio Code (version:1.70.2)
3. **Angular framework:** version 14.0.0
4. **Node.js version:** v16.3.1.
5. **Express.js version:** v4.18.1
6. **Web Browser:** Google Chrome (version 104.0.5112.81 (Official Build) (64-bit))
7. **Solid pod provider:** Inrupt.net [8]

[8] https://inrupt.net/[Accessed:17-08-2022]

Library name	Version	Command to install
@inrupt/solid-client	1.23.1	npm i @inrupt/solid-client
@inrupt/solid-client-authn-browser	1.12.0	npm i @inrupt/solid-client-authn-browser
@inrupt/vocab-common-rdf	1.0.5	npm i @inrupt/vocab-common-rdf

Table 4.1: solid Inrupt Javascript libraries

Node command	Action
npm init	creates node project and package.json
npm install express –save	downloads express library files and installs them

Table 4.2: Node setup commands

4.3.2 Initial setup

The working prototype is developed in the local machine with the development environment specifications mentioned in the section 4.3. Let us look into the initial setup of the development environment in the following section.

Angular setup

Node.js [9] and npm package manager were installed first as they are the basic requirements for installing Angular. The whole basic angular setup is done by following the official documentation of the Angular setup[30]. To avoid developing user interaction components like buttons, dropdown select, and date picker from the scratch Angular Material UI component library [10] is installed and used in this project. The Inrupt JavaScript libraries shown in the table 4.1are used to handle Solid related development and they are installed using npm in the Angular project created. Visual Studio Code is used as an IDE to code and navigates between files in the Angular project created.

Node.js setup

The backend server is Node.js with an Express.js server. Node.js which is installed already in the Angular setup 4.3.2is used to create a new node project. To create a node project, we create an empty directory as a first step and then the commands shown in 4.2 are executed sequentially in that directory. Finally, the Inrupt JavaScript libraries shown in the Table 4.1 is installed as the server directly interacts with the Inrupt pod provisioned for this project.

[9] https://nodejs.org/en/[Accessed:17-08-2022]

[10] https://material.angular.io/[Accessed:17-08-2022]

Account type	WebID
patient account	https://lokesh.inrupt.net/profile/cardme
third party account	https://asegroup.inrupt.net/profile/cardme
Representative account	https://solid-pcrv.inrupt.net/profile/cardme

Table 4.3: Inrupt.net Solid accounts

Inrupt Pod setup

To obtain the pod from Inrupt, the user has to sign up with Inrupt. After signing up, each user will be provided with a unique webID, pod profile and pod storage. For prototyping, four different Inrupt accounts were created and they are shown in the Table 4.3.

Development of User Interface and server functions

The development is done by addressing each functional requirement in the order it is defined in the section 3.4. The first and foremost implementation done while developing the application is User details management. This component is the key component in identifying and segregating users based on which the following screens are rendered for the user to view. The second component is the View Handler which composes of the router and individual screens that will be rendered based on the user logged in by identifying them through user details management.

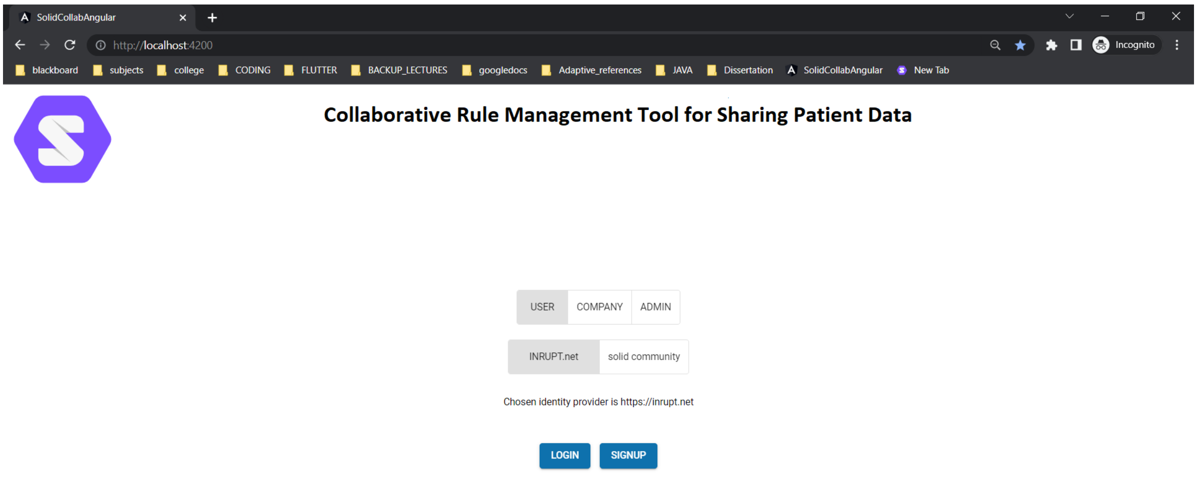
The backend is the Node.js express server where the controller is an "index.js" file that handles all the incoming requests to the server from the user interface implemented in Angular. The file "crudService.js" contains both the CRUD Handler and Data Transformer that is responsible for interacting with the Pods. The explanation of the development of the user interface and server functions in detail is not necessary as far as this report is concerned. All the details related to development (code and documents) are published on Github repo: `https://github.com/LokeshSelvakumar/dissertation_solid`.

4.3.3 User Interface

This section briefly discusses the development of user interface screens along with functionalities to satisfy the functional requirements identified in the section 3.4. There are total of five screens developed as a part of the proposed tool.

Login/Sign Up page

The Login/Sign Up page is shown in the Fig.4.3. This is the landing page of the application as soon the application URL is entered in the browser. This page is responsible for the Login and Sign Up functionalities related to the proposed application. A user can select the nature of the user (patient, third party or admin), select the pod provider in which they have an account already and sign up or log in to the collaborative rule management tool using this page.



Collaborative Rule Management Tool for Sharing Patient Data

Chosen identity provider is https://inrupt.net

Fig. 4.3: Login/Sign Up page

For simplicity and compatibility issues with Inrupt Javascript libraries, only two Solid Identity Providers are supported in the CRMT application developed (Inrupt.net and solid community). The authentication flow in the application is described in the Fig.??. The flow is described in [31] and it involves three steps:

1. Whenever the user clicks the Sign-Up or Login button in the CRMT application, the application starts the login process by sending the user to the user's Solid Identity Provider selected by the user on the login page.

2. The user logs in to the Solid Identity Provider

3. The Solid Identity Provider sends back the user to the CRMT application, where the CRMT application handles the returned authentication information to complete the login process.

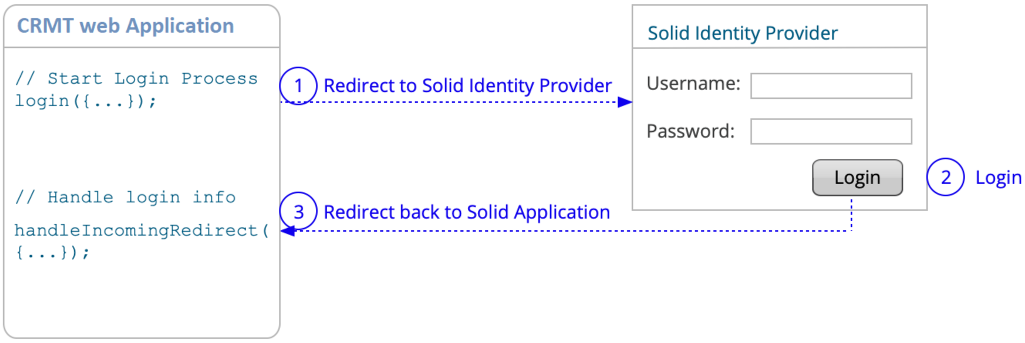
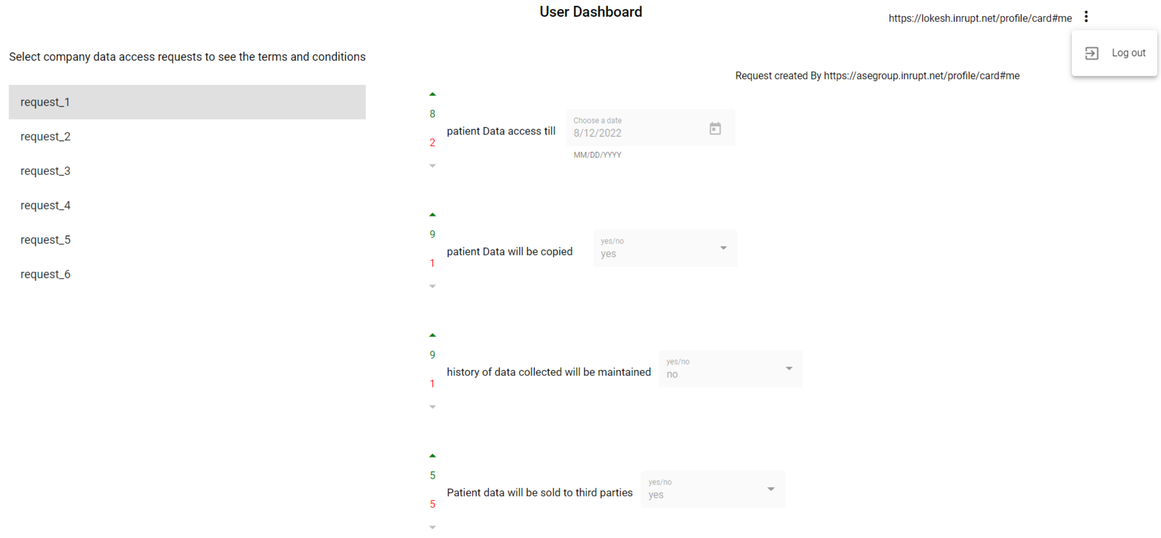


Fig. 4.4: Login Flow in the CRMT application

User Dashboard

The user dashboard is shown in the Fig.4.5. When a patient logs into the CRMT application successfully, he reaches the user dashboard page of the application which shows all the requests submitted by the third parties on the left side of the screen. The centre and right sides of the screen display the individual rules of the data access request selected on the left screen. Each rule has a voting button to its left through which the patients can upvote or downvote. There is a comment box present at the bottom of the screen through which the patients can comment and collaborate with each other. The user dashboard with comment box Fig.A1.3 is attached in the appendix A1



User Dashboard

https://lokesh.inrupt.net/profile/card#me

Log out

Select company data access requests to see the terms and conditions

- request_1
- request_2
- request_3
- request_4
- request_5
- request_6

Request created By https://asegroup.inrupt.net/profile/card#me

▲ 8 2 ▼ patient Data access till — Choose a date: 8/12/2022 (MM/DD/YYYY)

▲ 9 1 ▼ patient Data will be copied — yes/no: yes

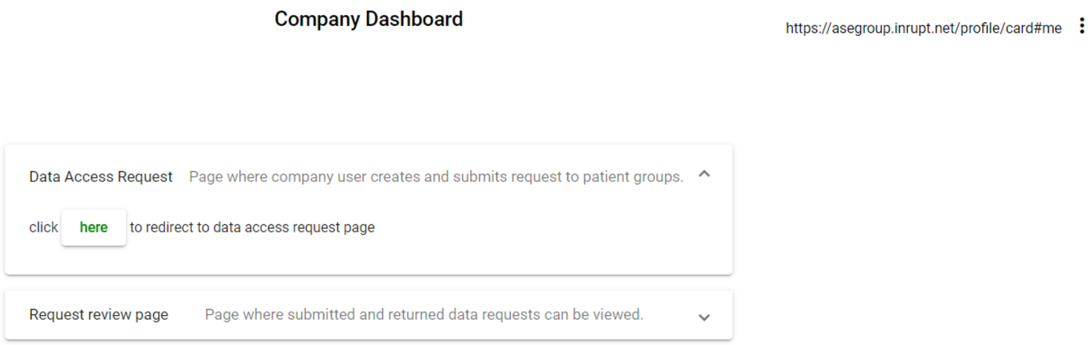
▲ 9 1 ▼ history of data collected will be maintained — yes/no: no

▲ 5 5 ▼ Patient data will be sold to third parties — yes/no: yes

Fig. 4.5: User Dashboard in CRMT application

Third-party Dashboard

When a third party who wishes to submit a data access request to the patient groups, logs into the CRMT application successfully, he is shown the company dashboard page. The company dashboard page provides two fluid expansion panels with descriptions on each panel indicating what can be found in it. The first panel packs a navigation button to take the user to the data access request creation page. The second panel provides a navigation button for the user to navigate to the review page where all the submitted requests can be reviewed. The third-party dashboard is shown in the Fig.4.6.



Company Dashboard

https://asegroup.inrupt.net/profile/card#me

Data Access Request Page where company user creates and submits request to patient groups.

click here to redirect to data access request page

Request review page Page where submitted and returned data requests can be viewed.

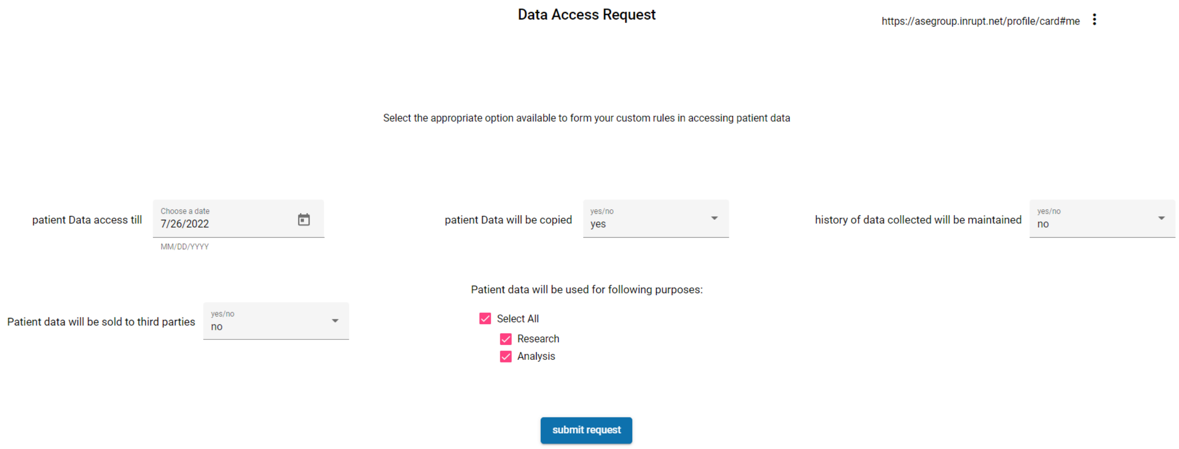
Fig. 4.6: Third-party Dashboard in CRMT application

Data Access Request Page

When a third party or company user clicks the button to navigate to the data access request page from the company dashboard screen, the data access request page is opened. This page is used to create data access requests by editing the rule template provided. The set of rules in this page are pre-defined and the user can only edit the rules by interacting with the dropdown select and data selection feature. The rules displayed here are taken from the section 3.7 which describes the purpose and how the rules are framed. The Data Access Request Page is shown in the Fig.4.7.

Administrator Dashboard

The representative dashboard or administrator dashboard is shown in the Fig.4.8. The representative of the patient groups is called an administrator because he has more authority over the CRMT application and he has access to all the features provided by the application.



Data Access Request

https://asegroup.inrupt.net/profile/card#me ⋮

Select the appropriate option available to form your custom rules in accessing patient data

patient Data access till — Choose a date: 7/26/2022 (MM/DD/YYYY)

patient Data will be copied — yes/no: yes

history of data collected will be maintained — yes/no: no

Patient data will be sold to third parties — yes/no: no

Patient data will be used for following purposes:

☑ Select All

☑ Research

☑ Analysis

Fig. 4.7: Data Access Request page in CRMT application

His sole responsibility is to monitor each request submitted by the third party. After a fixed cooling period, he checks for the upvotes and downvotes in each request and takes a decision on what to do with the request. With this page, the administrator can view the status of all the requests submitted to the patient groups by third parties along with the upvotes, downvotes and comments of the patients. Review, Accepted, Rejected, Resubmission rejected and Resubmission Accepted are the possible status of requests seen on this screen. The representative can accept, reject or edit and submit back the requests to the third party who created them using the action buttons provided at the bottom. Editing of the rules can be enabled and disabled by the action button provided on the top right-hand side.

the possible status of each request and its meaning:

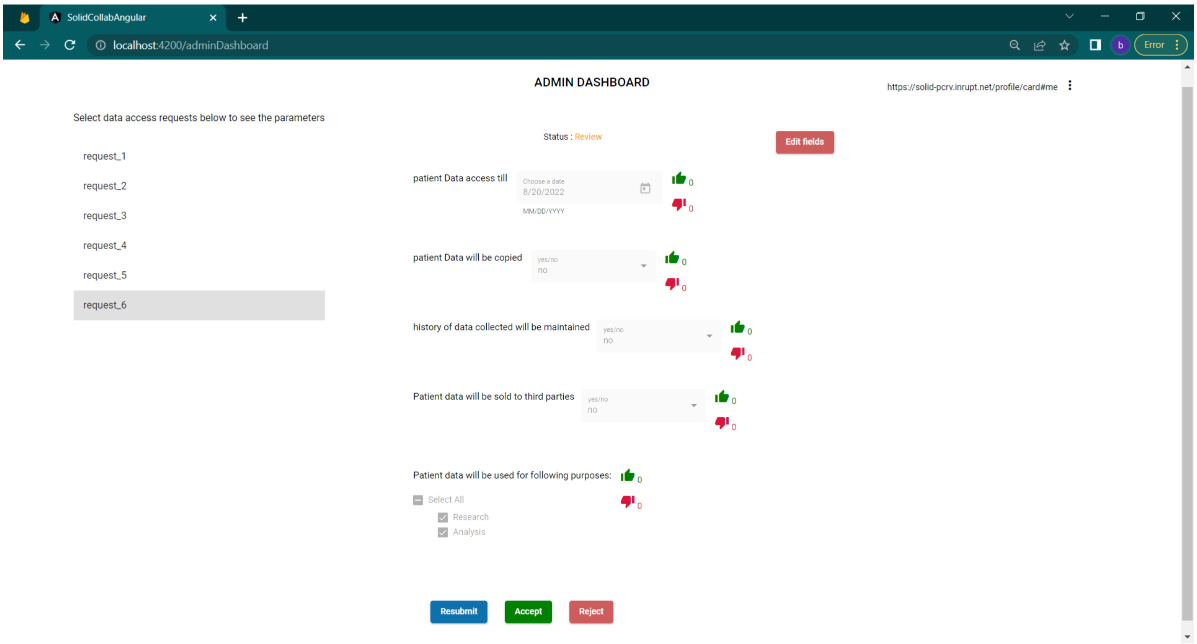
1. **Review:** the representative of the patient groups has not acted upon this request and the patient groups are still discussing the request.

2. **Accepted:** the representative of the patient groups accepts the requests as the request receives more upvotes and positive replies from the patients.

3. **Rejected:** the representative of the patient groups rejects the request as the request receives more downvotes and negative comments from the patients.

4. **Resubmission Rejected:** the representative edits the data access request rules and submits the edited request back to the third party. The request creator rejected it.

5. **Resubmission Accepted:** the representative edits the data access request and submits the edited request back to the third party. The request creator accepts it.



ADMIN DASHBOARD

Select data access requests below to see the parameters

Status : Review

patient Data access till: Choose a date 8/20/2022 MM/DD/YYYY 👍 0 👎 0

patient Data will be copied: yes/no no 👍 0 👎 0

history of data collected will be maintained: yes/no no 👍 0 👎 0

Patient data will be sold to third parties: yes/no no 👍 0 👎 0

Patient data will be used for following purposes: 👍 0 👎 0

- ☐ Select All
  - ☑ Research
  - ☑ Analysis

Fig. 4.8: Administrator Dashboard

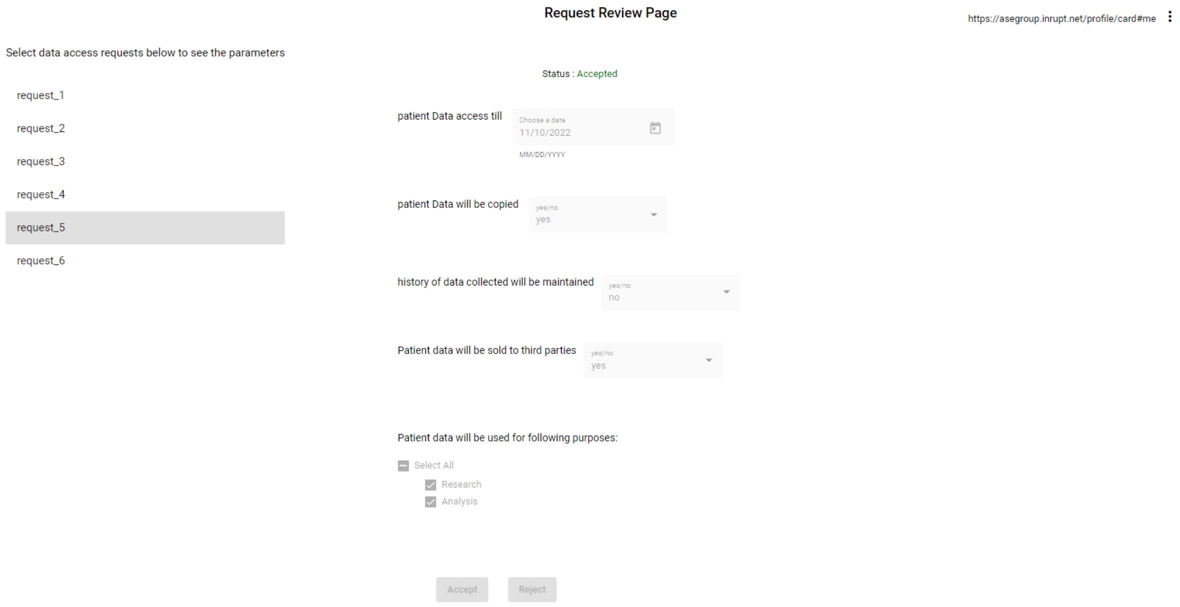
Request review page of third parties

The Request review page of third parties is shown in the Fig.4.9. When a third party or company user clicks the button to navigate to the request review page from the company dashboard screen, the request review page is opened. This page is used to view the submitted requests by the logged-in the third party. With this page, the user can view the status of all the requests submitted to the patient groups. Review, Accepted, Rejected, Resubmission rejected and Resubmission Accepted are the possible status of requests seen on this screen. Also, the third party can accept or reject the requests which are edited and submitted back by the representative of the patient groups on this screen with the help of buttons provided at the bottom.

4.3.4 Data Access Request Rules implementation

The rules framed from the section 3.7 is stored as an ODRL profile in the form of a knowledge graph in solid pod. The following code is the ODRL policy representation of how each request will be stored when all the rules are selected by the user on the data access request creation page.

```
@prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> .
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#> .
```



Request Review Page

https://asegroup.inrupt.net/profile/card#me

Select data access requests below to see the parameters

request_1

request_2

request_3

request_4

request_5

request_6

Status : Accepted

patient Data access till — Choose a date: 11/10/2022 (MM/DD/YYYY)

patient Data will be copied — yes/no: yes

history of data collected will be maintained — yes/no: no

Patient data will be sold to third parties — yes/no: yes

Patient data will be used for following purposes:

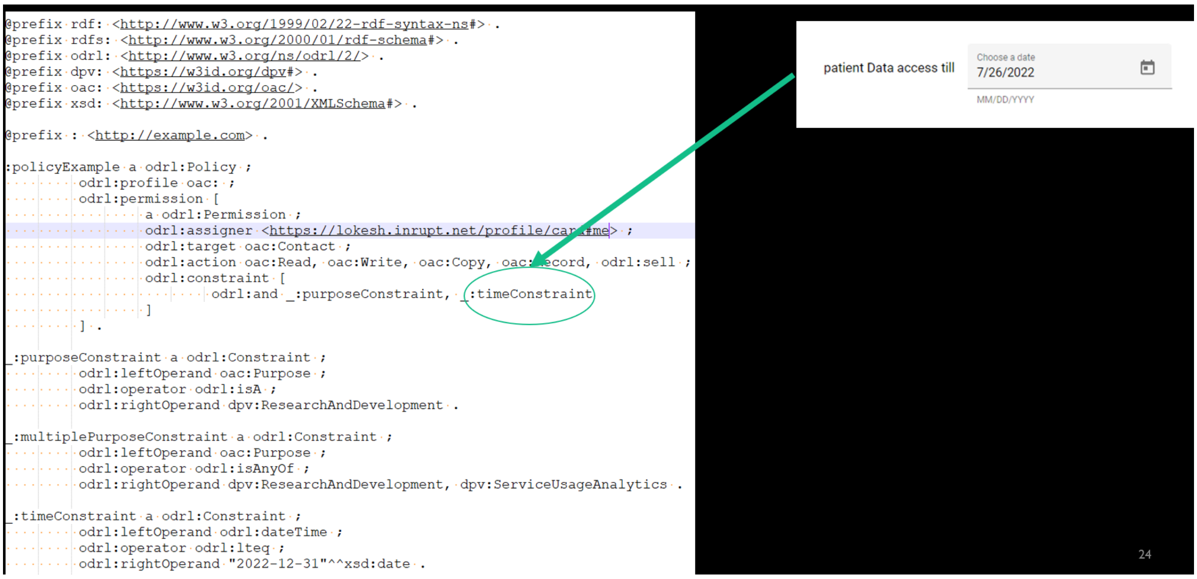
- ▬ Select All
  - ☑ Research
  - ☑ Analysis

Fig. 4.9: Request Review Page in CRMT application

```
@prefix odrl: <http://www.w3.org/ns/odrl/2/> .
@prefix dpv: <https://w3id.org/dpv#> .
@prefix oac: <https://w3id.org/oac/> .
@prefix xsd: <http://www.w3.org/2001/XMLSchema#> .
@prefix : <http://example.com> .

:policyExample a odrl:Policy ;
         odrl:profile oac: ;
         odrl:permission [
            a odrl:Permission ;
            odrl:assigner <https://lokesh.inrupt.net/profile/card#me> ;
            odrl:target oac:Contact ;
            odrl:action oac:Read, oac:Write, oac:Copy, oac:Record, odrl:sell ;
            odrl:constraint [
                         odrl:and _:purposeConstraint, _:timeConstraint
                            ]
                        ] .

_:purposeConstraint a odrl:Constraint ;
         odrl:leftOperand oac:Purpose ;
         odrl:operator odrl:isA ;
```

```
        odrl:rightOperand dpv:ResearchAndDevelopment .

_:multiplePurposeConstraint a odrl:Constraint ;
        odrl:leftOperand oac:Purpose ;
        odrl:operator odrl:isAnyOf ;
        odrl:rightOperand dpv:ResearchAndDevelopment, dpv:ServiceUsageAnalytics .

_:timeConstraint a odrl:Constraint ;
        odrl:leftOperand odrl:dateTime ;
        odrl:operator odrl:lteq ;
        odrl:rightOperand "2022-12-31"^^xsd:date .
```

For example, a request creator identified by
WebID https://lokesh.inrupt.net/profile/card#me, when selecting a date in the first rule framed in the section 3.7 (Patient data access till 2022-12-31) will create a policy with odrl:assigner equals to <https://lokesh.inrupt.net/profile/card#me> and the date will be stored as _:timeConstraint (an odrl constraint) as mentioned in the Fig.4.10. All the other rules and the reference to how it is stored in the ODRL policy can be found in the figures (Fig.A1.6,Fig.A1.7,Fig.A1.8,Fig.A1.9) attached in the Appendix A1.



```
@prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> .
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#> .
@prefix odrl: <http://www.w3.org/ns/odrl/2/> .
@prefix dpv: <https://w3id.org/dpv#> .
@prefix oac: <https://w3id.org/oac/> .
@prefix xsd: <http://www.w3.org/2001/XMLSchema#> .

@prefix : <http://example.com> .

:policyExample a odrl:Policy ;
        odrl:profile oac: ;
        odrl:permission [
                a odrl:Permission ;
                odrl:assigner <https://lokesh.inrupt.net/profile/card#me> ;
                odrl:target oac:Contact ;
                odrl:action oac:Read, oac:Write, oac:Copy, oac:Record, odrl:sell ;
                odrl:constraint [
                        odrl:and _:purposeConstraint, _:timeConstraint
                ]
        ] .

_:purposeConstraint a odrl:Constraint ;
        odrl:leftOperand oac:Purpose ;
        odrl:operator odrl:isA ;
        odrl:rightOperand dpv:ResearchAndDevelopment .

_:multiplePurposeConstraint a odrl:Constraint ;
        odrl:leftOperand oac:Purpose ;
        odrl:operator odrl:isAnyOf ;
        odrl:rightOperand dpv:ResearchAndDevelopment, dpv:ServiceUsageAnalytics .

_:timeConstraint a odrl:Constraint ;
        odrl:leftOperand odrl:dateTime ;
        odrl:operator odrl:lteq ;
        odrl:rightOperand "2022-12-31"^^xsd:date .
```

patient Data access till

Choose a date
7/26/2022
MM/DD/YYYY

Fig. 4.10: An example of ODRL policy generated

4.4 Summary of Implementation

The technical implementation is the hardest part in the research which consumed a considerable amount of time in this research. It started with developing the tool to satisfy Functional Requirement 1 and then stopped with Functional Requirement 6. The voting component is a new component developed from scratch which is a by-product of this research. The implementation of comment feature as a collaborative feature in the tool is completed at the server side, however it is yet to be implemented in the user interface. The research papers [32], [29] and the official documentation from Inrupt [33] provided most of the insights and implementation techniques needed for this chapter.

5 Evaluation

This chapter starts with the non-goals of this research project to clearly outline the parts that are beyond the scope of this research and then highlight the evaluation of the patient data collaborative rule management tool developed as a part of this research which acts as a solution to the problem addressed in this research.

5.1 Non-goals

This section clearly clarifies the non-goals of this research.

- This research is not intended to present a comprehensive reference to the Solid platform which is used to build the application. While we use Solid to provide a solution for our research question, the study is not exhaustive, and definitely not an in-depth analysis of Solid as it is beyond the scope of the research.
- I have studied the technical aspects of Solid to the extent required to build the collaborative rule management tool proposed. Though good standards of coding practices are carried out while building the application, performance and maintainability are not the focus of the development.
- The software tool developed is a prototype and serves as a proof-of-concept demonstrating the capabilities rather than a production-ready system. Therefore, user experience evaluation is not done as a part of this research because patient groups need to be identified and educated to make them understand the solid and the CRMT tool developed in this research.
- This research does not deal with any real-time data of the patients or any individuals as the main motive is to develop the application as a collaborative medium and the use of real-time health information is beyond the scope of this research. Therefore, there is neither data analysis nor data set preparation involved in this research.

5.2 Security Considerations

All applications or servers available online have the risk of being attacked. Though the application is not production ready, the personalised web data servers involved in this project will hold the patient groups' private health information. This brings a lot of security and privacy concerns related to the data. Because when the data is compromised the identity and medical history of the patient are exposed which can be considered a breach of privacy. Some of the common threats to the solid ecosystem and solutions are discussed below.

1. **Distributed denial of service (DDoS) attack:** This is a type of attack targeted to flood the destination server thereby making it utilize all of its resources. Any legitimate request from the customer cannot be processed by the server. This type of attack is usually targeted to stop the service and bring it down. Any online site or service is inevitable to DDoS attacks. The DDoS attack can be prevented if the defence system has more resources than the attacker or it has good protection services like Cloudflare.
2. **Eavesdropping attack:** Since all the Solid applications are accessed via a web browser, the user has to be careful when using the application on a public network as they are easy targets for eavesdropping attacks. An eavesdropper can easily monitor network traffic on public networks and steal login credentials. In this case, if an eavesdropper gets the credential to the login identity provider, then all the Pods that are accessible using the WebID are compromised.
3. **Browser based attacks:**Since all the pods and Solid based applications are accessed through the browser, once the browser is compromised, everything is compromised. So all browser-based attacks should be considered and protective measures should be taken against them.

5.2.1 Pod Providers and security

The existing Pod providers for Solid developers and users are Inrupt Pod spaces, inrupt.net, solidcommunity.net, solidweb.org, and trinpod.us. Inrupt Pod spaces secure the systems with auditing, end-to-end TLS encryption and OIDC/OAuth access control features. It also provides native monitoring, distributed logging, and backup and restores options. It also provides enterprise versions of Pod services. The inrupt.net is the older version of Inrupt Pod spaces with limited security and stability. Performance is also limited.

Both the solidcommunity.net and solidweb.org Pod providers are just a prototype implementation of the Solid server. They are fully functional servers however they lack security and stability. The solidcommunity.net is best suitable for developers and some early users to get used to the Solid ecosystem.

The trinpod.us is a second secure option which uses WebID that verifies the identities of users in order to give them a secure user experience. For storing the data, trinpod.us internally uses Amazon storage. Amazon being the number one cloud provider is a reliable, scalable, and secure place for storing data.

So, choosing a Pod provider determines how secure the data is. However, one can take complete control of the security and data privacy by self-hosting their own pod as solid provides a way to self-host. But this requires some technical knowledge, and it is not a user-friendly option yet.

5.3 Privacy considerations

As ambitions for a more digital healthcare system progress, this means that large volumes of health data will be available to use and exchange electronically. There is currently no overarching regulatory framework in place in Ireland to facilitate the safe and effective use of personal data in health and social care. Individuals also expect healthcare professionals and organizations to efficiently interact with one another and use their data to manage and administer the health system. However, there must be clarity about when and how health and social care providers can acquire, utilize, and share personal information. Additionally, sufficient security procedures must be promoted to defend against known and prospective threats connected with collecting, using, and sharing electronic health records (EHRs).

5.3.1 Migrating Data

When a user or patient wants to leave the Solid provider, the user can take or migrate the data to another Pod provider unless the current Pod provider doesn't allow it. So, the terms and conditions of individual Pod providers must be carefully read before choosing it. Since the data stored in Solid Pods is structured and according to Linked Data principles, Pod providers are completely neutral regarding the Pod content. The same structure should be supported by any Pod provider.

5.3.2 Third parties Replicating Data

Though we can restrict who has access to what part of the data, once the data is shared with the application, we cannot restrict the application or the user to duplicate the data. However, at any point in time, users can revoke access to the application. Also, the data that is already duplicated cannot be deleted however the data sharing preferences at any point can be controlled by the user. Once revoked, the application can no longer update the copy of the data it holds.

5.3.3 Deleting Pods and WebID

Anyone can leave Solid at any time by deleting their Pods from the Pod provider and WebID from the identity provider. The key thing to consider here is to delete the Pods before deleting the websites from the identity provider. Deleting WebID first will lock you out of Pods that need WebIDs to access it.

5.3.4 Data storage place and Law

Based on the law of the countries in which the hosting provider operates, pod providers have obligations to the individuals and legal entities to whom they provide services. The law establishes the government's authority to track and control illegal activity. The patient's or user's decision of where to keep their Pod determines which jurisdiction has supervision of the data in that Pod, unless the user is in Europe, in which case the General Data Protection Regulation applies regardless of the location of the Pod.

5.3.5 Data Integrity issues

The solid specification has a "trusted apps" feature which is new, and it has a weakness for origin validation. When a user grants access to their Pod to a Solid online app, the app Origin is added to the user's trusted apps list. The app is then given a token that allows it to interact with the Pod on the user's behalf, with just the Origin contained in those interactions being confirmed using the trusted applications list. Although typical browsers provide the Origin in HTTPS queries by default, a non-browser client is not obligated to do so. This means that anyone with access to the Origin-based token can evade Origin validation for the Pod using non-browser clients.

5.4 Complexity in the movement of diversified Patient groups' health information to Solid Pod

Based on the findings from the landscape of health information in the section 2.3 , it can be seen that the patient records are available in different formats and it also involves pictures, documents, scan records etc. The solid supports all formats of file storage as mentioned before however storing all the patient groups' health information is not done in this research. The storing of different data formats is not complex, however, the movement of diversified patient groups' data to the solid pod is a complexity. This complexity is not addressed in this research as it is beyond the scope of the research.

5.5 How far the use cases and goals are achieved?

The tool makes the patient collaborate with themselves by providing features that enable patients to upvote and downvote each rule to express their interests. Through this tool, the third parties can submit their data access requests to patient groups and also the tool enables the representative of the patient groups to reject or submit back the request. Thus the tool helps patient groups, their representative and third parties collectively agree to the common rules in sharing, using and accessing the health information of the patient groups.

Initially, Access Control List (ACL) was used to encode the rules of the data access request but it lacks features to express more complicated rules. Therefore, the Open Digital Rights Language (ODRL) ontology [29] as a policy expression language is used to create ODRL profiles to express the rules governing the data access in this research. This made the rules more expressive and vocabulary for user interaction is added as an extension to the existing ODRL profiles.

The tool lacks efficiency and speed involving CRUD operations as each update and retrieval of data is very slow compared to conventional databases like MySQL, PostgreSQL, Firebase etc. Although the data access requests are encoded in the knowledge graph as ODRL profiles in solid pods, further research is needed in replacing the Access Control List(ACL) of Solid pods with ODRL profiles to complete the ultimate goal of this research. The Patient Data Collaborative rule management tool can act as a baseline for any software application built to achieve the same goal in the future.

Adding more rules

5.6 Scalability and Extensibility

The user interface is developed in Angular and it is written in such a way that it is extensible and easily scalable. Angular itself is known for its scalability, however, the components and functionalities are developed in a manner that it is easy to add any number of components. The node server is also scalable because the functionalities are abstracted and isolated. All the functionalities are extensible. When there are more users using the application, a load balancer can be implemented and multiple clones of the application can be deployed making each instance handle specific functionalities. The development time to improve scalability is a little and a highly effective strategy. Other strategies like decomposing and splitting can also be employed to make the node server scalable.

The storage space limitation of Pods depends on the Pod provider and no information on this is found in any of the documentation. However, Inrupt.net provides Enterprise Solid Server (ESS) which has many premium services like scalability, advanced security, monitoring etc. In terms of the CRMT application, the application saves all the data in the Patient group pod and the third party pod. So, the system as a whole is scalable.

Adding more ODRL rules for new granular rules framed in the future can be done which makes the application extensible, however, it involves writing complex lines of code to create the ODRL nested triple. Irrespective of the patient data stored in a personal Pod or a community Pod, the same system architecture will work with little changes in the Pod settings that are configured in the backend server. The ODRL policy generated can also be stored in the GraphDB as an alternative to storing it in the Pod directly. However, when the granular rules have to be enforced on the Pod when accepted by all the parties involved, it has to be available in the Pod to make it work.

5.7 Challenges

The following are some of the challenges faced in this research:

- As a complete beginner to the entire Solid ecosystem, it took me a great deal of time in understanding the prerequisites like Solid, Pods and the Inrupt JavaScript libraries.
- Since there was no previous work on Angular with Inrupt JavaScript libraries and Node.js, I had to solve the technical problems faced during the implementation on my own which consumed a lot of time than usual. The solid community is less active and still growing which offers minimal support to technical problems.

- The lines of code to cover a single use case are very extensive as the existing libraries lack features like updating a nested Thing without updating the whole object. The development time is more as the lines of code to cover a single use case becomes extensive when Knowledge Graph is involved.
- While the ODRL profile used increases the expressiveness of policies, one can argue that these policies, when used to represent real-world use-cases, might become too complex.
- Users or patient groups should be educated on solid, pods and how to use the tool.

6 Conclusion and Future work

6.0.1 Conclusion

This research aimed to identify solutions to enable patient groups collectively manage their health information thereby enabling them to control who has access to the information by granular access control. The whole research project is carried out in four phases as mentioned in the research approach in the section 1.3. Firstly, the current landscape of Ireland's health information and surveys to understand public mentality on health information are studied and the initial research question is framed. Survey findings indicated that the majority of the patients are ready to share their medical information with third parties however they feel more involved and empowered when they can see who has access to their medical information. Though patients have the right to view their medical data, it is always not an easy process. The research question is refined at this point and Key objectives from the research question are identified. Solid, the technology that has privacy and data ownership at its heart was seen as a potential area and the state of the art of Solid was studied. The advantages and disadvantages of implementing Solid were studied. As an alternative to the conventional databases and also as an initiative toward the semantic web, Solid Pods are found to be the perfect fit for this research. The only downside to implementing Solid was the steep learning curve. Secondly, the existing rules for data sharing platforms were analysed and compared. Thirdly, to solve the research problem undertaken in this research, a software application is proposed which involves the interaction of Solid, and Semantic web and linked data. Therefore, the research areas namely health information landscape in Ireland, Solid, and Semantic web and linked data are the three fields interacting in this particular study Each area is studied. Fourthly, designing of the whole system is done which involves identifying actors external to the system boundary, analysing use cases relevant to the system boundary, identifying functional requirements and designing functional architecture. Finally, the implementation of the design, thereby developing the proposed tool, a Solid-Powered Collaborative Rule Management Tool (CRMT) for sharing patient data.

The CRMT application is a local application which is developed as a proof-of-concept and therefore not production ready. The real-time testing of the application needs to be performed to understand the real-time complexity involved. The application covers all the functional requirements identified and use cases identified. However, the comment functionality is not realised in the user interface due to time constraints. Though the application stores data access request as ODRL policies in the Pod, it does not enforce the Pod to use the ODRL policies. This implementation is yet to be done to realise the ultimate goal of helping patient groups control their data stored in the Pod. This research can be seen as one of the three steps needed to attain the goal of enabling patient groups to control their data. Movement of diversified patient groups data to the Solid Pods and implementing reasoner to replace ACL with ODRL policies are the other two separate steps that need to be done which are beyond the scope of this research. Although the ODRL policy is a previous work [29], vocabulary for adding collaborative information like votes and comments is introduced in it to make it extensible. Though the ODRL policy defined here is for health information, the ODLR policy itself is an open standard. It can be used by companies all around the world in a lot of different communities for a different category of data altogether. To conclude, the developed tool CRMT for patient data sharing is a successful working prototype that can help patients and third parties collaborate to agree on the granular rules for access control and also encode granular access control rules for data access in the form of ODRL policies which is stored in the patient groups' Pod.

6.0.2 Future work

The following are the future work that can be done to extend this research:

1. Although the software tool is built using a single knowledge graph, multiple ontologies can be used to build the same thereby eliminating the nested triples and their intensely complicated structure.

2. The speed and efficiency of the CRMT application can be optimized by adding another database to handle tool-related data like login, sign up, and patient collaboration data (up votes, down votes, comments) thereby isolating ODRL profiles from the tool-related data making it efficient and less complicated.

3. Improvements can be made in the CRMT tool like enhancements in User Interface (UI), the addition of new features in the user interface like displaying the history of all the edited rules in each request. Improving the information stored in the Pod with two Knowledge Graphs.

4. This tool can act as a baseline where tools built using different technologies can be compared with this one.
5. Movement of diversified patient data to the Solid Pods by educating People about Solid and its ecosystem which promotes semantic web and Linked Data.

Bibliography

[1] Rob Reinhardt, "Technology Tutor: Why counselors need to understand health information exchange," 2018. https://ct.counseling.org/2018/06/technology-tutor-why-counselors-need-to-understand-health-information-exchange/.

[2] C. Massimo, S. Henk, M. Marina, H. Jiri, C. Igor, L. Steven, P. Marisa, and B. Jaap, "Digitranscope: The governance of digitally-transformed society," *EUR 30590 EN, Publications Office of the European Union, Luxembourg*, 2021.

[3] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *EASE '14*, 2014.

[4] "The Need to Reform Ireland's National Health Information System," 2021. https://www.hiqa.ie/sites/default/files/2021-10/The-need-for-reform-of-the-health-information-system.pdf.

[5] Brendan Walsh, Ciarán Mac Domhnaill and Gretta Mohan, "Developments in healthcare information systems in Ireland and internationally," 2021. https://www.esri.ie/system/files/publications/SUSTAT105_0.pdf.

[6] "Health act of 2007," 2021. https://www-irishstatutebook-ie.elib.tcd.ie/eli/2007/act/23/enacted/en/html.

[7] D. Ivankovic, T. Jansen van Eijndt, E. Barbazza, Brito Fernandes, N. Klazinga, and D. Kringos Pereira Martins, "Status of the health information system in ireland and its fitness to support health system performance assessment: A multimethod assessment based on stakeholder involvement," 03 2022.

[8] Irish Platform for Patient Organisations, Science and Industry, "Verdict from a citizens' jury on access to health information," 2021. https://www.ipposi.ie/wp-content/uploads/2021/09/IPPOSI_CJury_Full_Report_06092021.pdf.

[9] B. W. Schermer, B. Custers, and S. van der Hof, "The crisis of consent: how stronger legal protection may lead to weaker consent in data protection," *Ethics and Information Technology*, vol. 16, pp. 171–182, 2014.

[10] "General Data Protection Regulation (GDPR) consent," 2018. https://gdpr-info.eu/issues/consent/.

[11] "General data protection regulation (gdpr) art. 4 gdpr definitions." https://gdpr.eu/article-4-definitions/.

[12] H. R. B. (HRB), "Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations," 2018. https://www.hrb.ie/funding/gdpr-guidance-for-researchers/gdpr-and-healthresearch/health-research-regulations-2018/.

[13] "General Data Protection Regulation (GDPR)," 2018. https://gdpr.eu/tag/chapter-1/.

[14] Irish Platform for Patient Organisations, Science and Industry, "The patient perspective on access to health information results from a 2021 survey," 2021. https://www.ipposi.ie/wp-content/uploads/2021/12/Patient-survey-report-final-compressed.pdf.

[15] Health Information and Quality Authority, Department of Health, Health Service Executive, "Findings from the National Public Engagement on Health Information 2020 - 2021," 2021. https://www.hiqa.ie/sites/default/files/2021-09/Findings-from-the-National-Public-Engagement-on-Health-Information.pdf.

[16] "Freedom of information act," 2014. https://www.irishstatutebook.ie/eli/2014/act/30/enacted/en/html.

[17] "Data Protection Act," 2018. https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html.

[18] T. Berners-Lee, J. Hendler, and O. Lassila, "The semantic web," *Scientific American*, vol. 284, no. 5, pp. 34–43, 2001.

[19] C. Bizer, T. Heath, and T. Berners-Lee, "Linked data: The story so far," *International Journal on Semantic Web and Information Systems*, vol. 5, pp. 1–22, 07 2009.

[20] "Solid," https://solid.mit.edu/.

[21] "C-Accel 2019 Glossary," 2019. https://github.com/C-Accel2019/Glossary/blob/master/glossary.md#Knowledge-Graph-KG.

[22] T. Berners-Lee and R. Verborgh, "Solid: Linked data for personal data management," 2018. https://rubenverborgh.github.io/Solid-DeSemWeb-2018/.

[23] "Solid specification." https://github.com/solid/solid-spec/tree/103b1e027356bd525e4cad0138e8288f4881df39#webid-tls.

[24] "Rdf 1.1 primer," 2014. https://www.w3.org/TR/2014/NOTE-rdf11-primer-20140624/.

[25] E. Kalemi and E. Martiri, "Foaf-academic ontology: A vocabulary for the academic community," in *2011 Third International Conference on Intelligent Networking and Collaborative Systems*, pp. 440–445, 2011.

[26] "Solid : Web access control (wac)." https://solid.github.io/web-access-control-spec/.

[27] "Linked data notifications : W3c recommendation," 2017. https://www.w3.org/TR/2017/REC-ldn-20170502/.

[28] "How to access your personal data under the GDPR." https://www.citizensinformation.ie/en/government_in_ireland/data_protection/rights_under_general_data_protection_regulation.html.

[29] B. Esteves, H. J. Pandit, and V. Rodríguez-Doncel, "Odrl profile for expressing consent through granular access control policies in solid," in *2021 IEEE European Symposium on Security and Privacy Workshops (EuroSPW)*, pp. 298–306, 2021.

[30] "Angular - setting up the local environment and workspace," https://angular.io/guide/setup-local.

[31] "Inrupt authentication flow." https://docs.inrupt.com/developer-tools/javascript/client-libraries/authentication/.

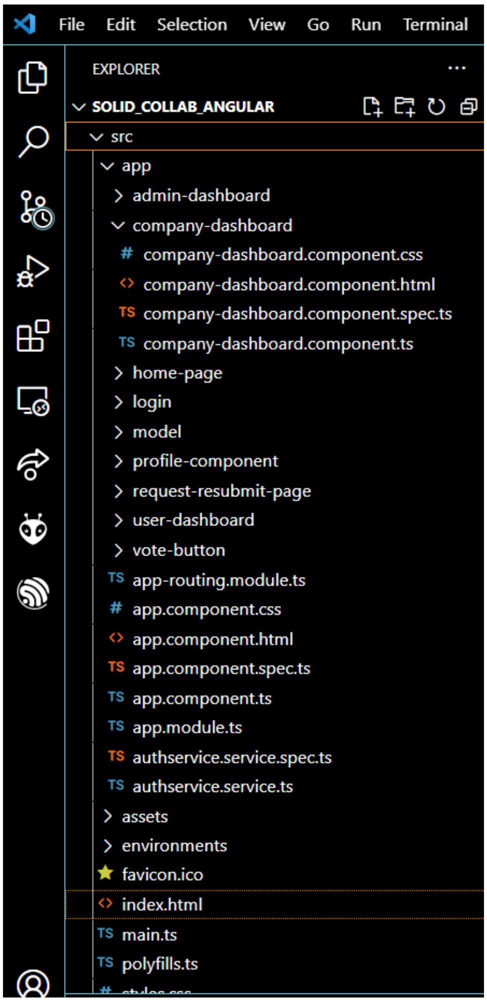
[32] "A solid-powered decentralised social network for academics: An evaluation of key considerations for developing practical solid-powered applications," 2019. https://www.scss.tcd.ie/publications/theses/diss/2019/TCD-SCSS-DISSERTATION-2019-046.pdf.

[33] "Inrupt javascript client libraries." https://docs.inrupt.com/developer-tools/javascript/client-libraries/.

A1 Appendix

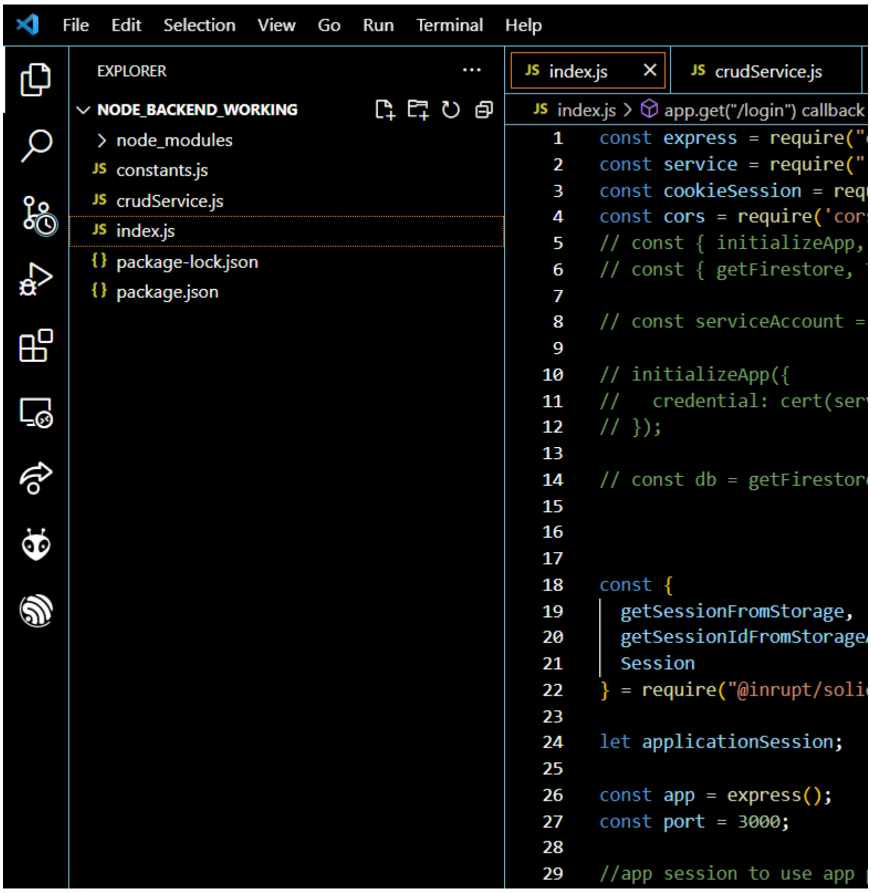
These are the screenshots of the project structure seen from the VSS code.

Fig. A1.1: Angular project structure in VSS code

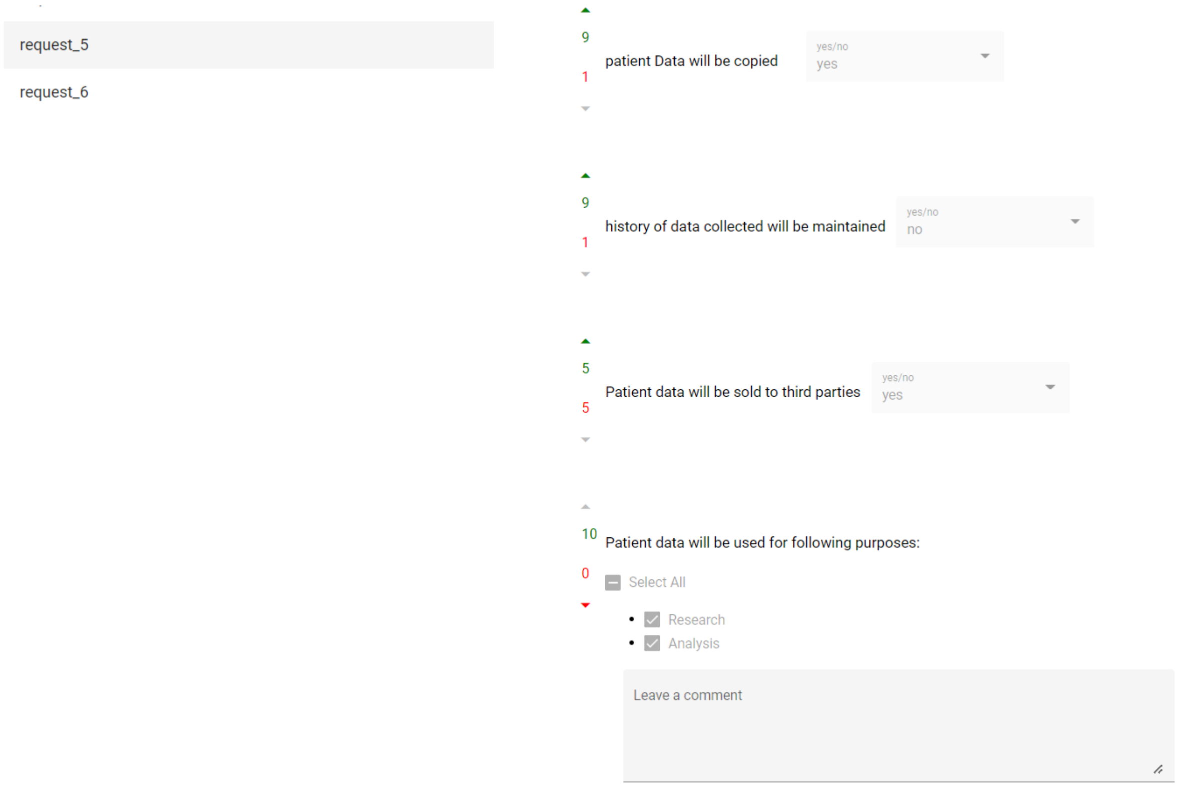


```
SOLID_COLLAB_ANGULAR
  src
    app
      admin-dashboard
      company-dashboard
        company-dashboard.component.css
        company-dashboard.component.html
        company-dashboard.component.spec.ts
        company-dashboard.component.ts
      home-page
      login
      model
      profile-component
      request-resubmit-page
      user-dashboard
      vote-button
      app-routing.module.ts
      app.component.css
      app.component.html
      app.component.spec.ts
      app.component.ts
      app.module.ts
      authservice.service.spec.ts
      authservice.service.ts
    assets
    environments
    favicon.ico
    index.html
    main.ts
    polyfills.ts
    styles.css
```

Fig. A1.2: Node.js project structure in VSS code



```
const express = require("
const service = require("
const cookieSession = req
const cors = require('cor
// const { initializeApp,
// const { getFirestore,

// const serviceAccount =

// initializeApp({
//   credential: cert(ser
// });

// const db = getFirestor



const {
  getSessionFromStorage,
  getSessionIdFromStorage
  Session
} = require("@inrupt/soli

let applicationSession;

const app = express();
const port = 3000;

//app session to use app
```



request_5

request_6

9
1
patient Data will be copied — yes/no: yes

9
1
history of data collected will be maintained — yes/no: no

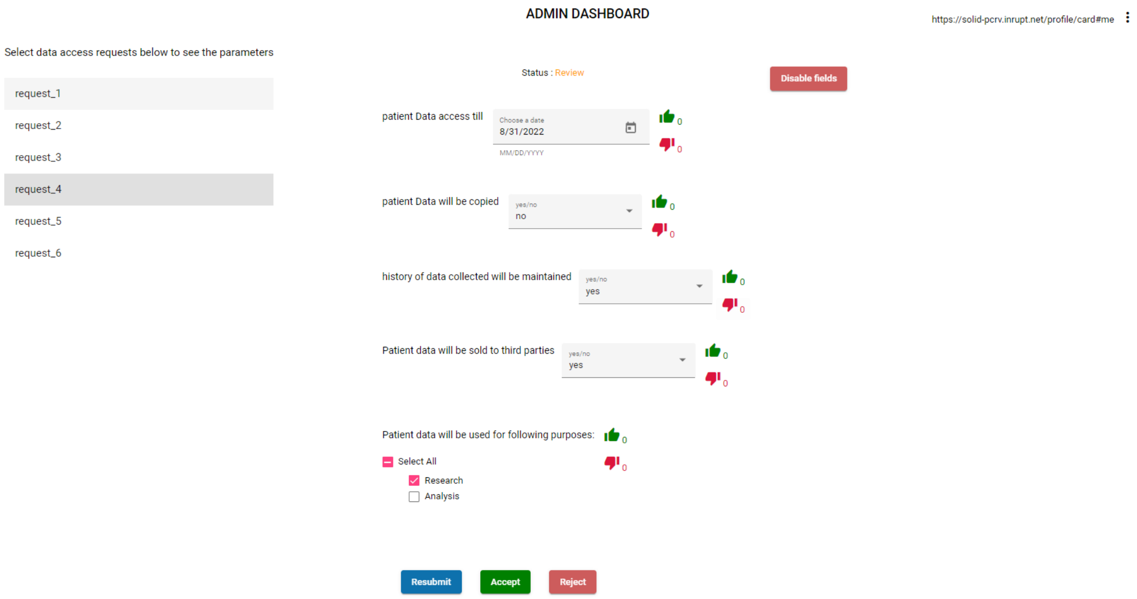
5
5
Patient data will be sold to third parties — yes/no: yes

10
0
Patient data will be used for following purposes:

- Select All
  - ☑ Research
  - ☑ Analysis

Leave a comment

Fig. A1.3: User Dashboard in CRMT application with comment box



ADMIN DASHBOARD

https://solid-pcrv.inrupt.net/profile/card#me

Select data access requests below to see the parameters

request_1
request_2
request_3
request_4
request_5
request_6

Status : Review

patient Data access till — Choose a date: 8/31/2022 (MM/DD/YYYY) — 0 0

patient Data will be copied — yes/no: no — 0 0

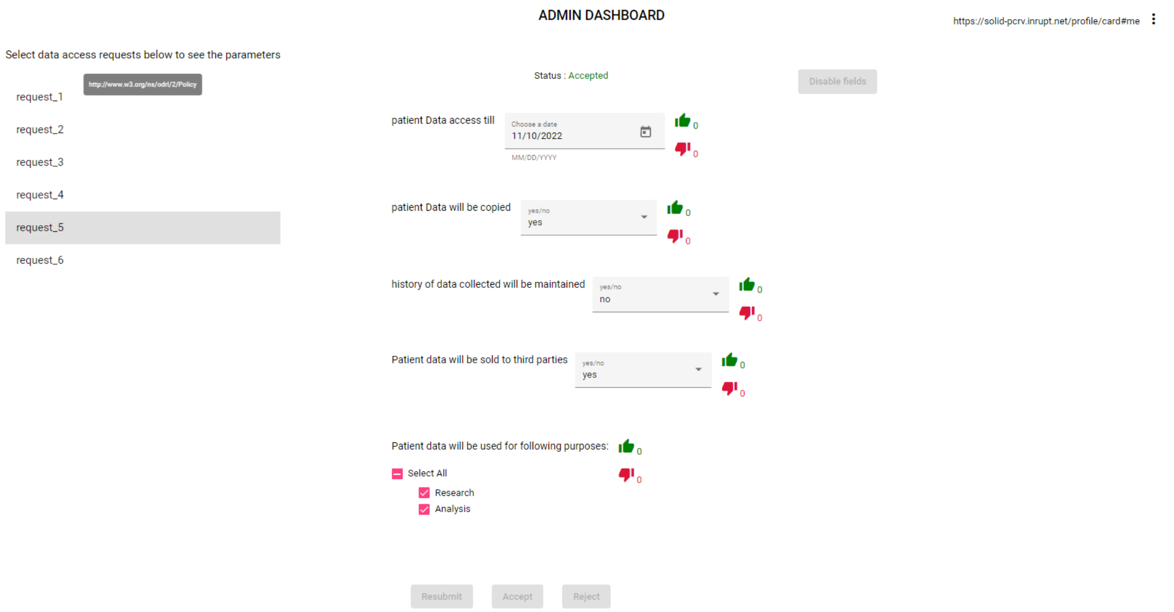
history of data collected will be maintained — yes/no: yes — 0 0

Patient data will be sold to third parties — yes/no: yes — 0 0

Patient data will be used for following purposes: — 0 0

- Select All
  - ☑ Research
  - □ Analysis

Fig. A1.4: Admin Dasboard in CRMT application with Review status



ADMIN DASHBOARD

https://solid-pcrv.inrupt.net/profile/card#me

Select data access requests below to see the parameters

- request_1
- request_2
- request_3
- request_4
- request_5
- request_6

Status : Accepted

patient Data access till: Choose a date 11/10/2022 (MM/DD/YYYY) 👍 0 👎 0

patient Data will be copied: yes/no yes 👍 0 👎 0

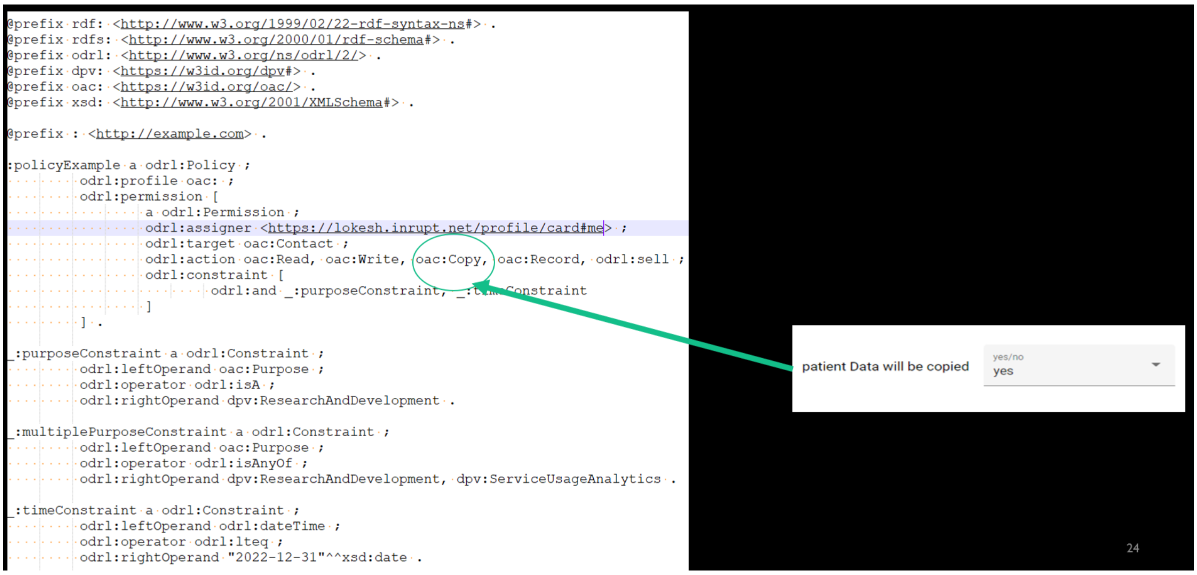
history of data collected will be maintained: yes/no no 👍 0 👎 0

Patient data will be sold to third parties: yes/no yes 👍 0 👎 0

Patient data will be used for following purposes: 👍 0 👎 0

- ☐ Select All
  - ☑ Research
  - ☑ Analysis

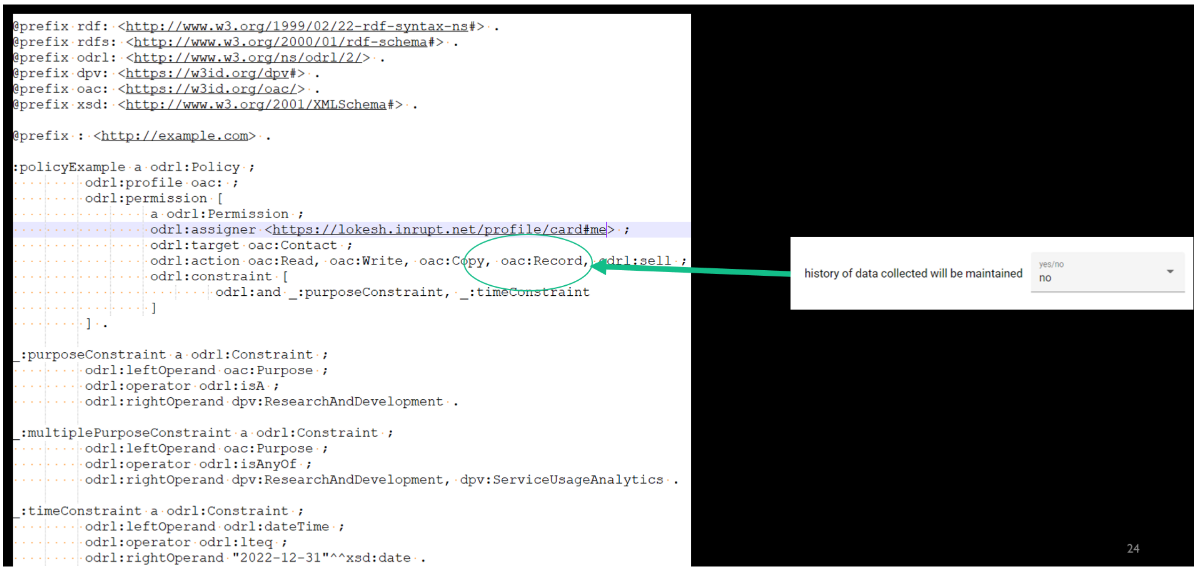
Fig. A1.5: Admin Dasboard in CRMT application with Accepted status



```
@prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> .
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#> .
@prefix odrl: <http://www.w3.org/ns/odrl/2/> .
@prefix dpv: <https://w3id.org/dpv#> .
@prefix oac: <https://w3id.org/oac/> .
@prefix xsd: <http://www.w3.org/2001/XMLSchema#> .

@prefix : <http://example.com> .

:policyExample a odrl:Policy ;
        odrl:profile oac: ;
        odrl:permission [
                a odrl:Permission ;
                odrl:assigner <https://lokesh.inrupt.net/profile/card#me> ;
                odrl:target oac:Contact ;
                odrl:action oac:Read, oac:Write, oac:Copy, oac:Record, odrl:sell ;
                odrl:constraint [
                        odrl:and _:purposeConstraint, _:timeConstraint
                ]
        ] .

_:purposeConstraint a odrl:Constraint ;
        odrl:leftOperand oac:Purpose ;
        odrl:operator odrl:isA ;
        odrl:rightOperand dpv:ResearchAndDevelopment .

_:multiplePurposeConstraint a odrl:Constraint ;
        odrl:leftOperand oac:Purpose ;
        odrl:operator odrl:isAnyOf ;
        odrl:rightOperand dpv:ResearchAndDevelopment, dpv:ServiceUsageAnalytics .

_:timeConstraint a odrl:Constraint ;
        odrl:leftOperand odrl:dateTime ;
        odrl:operator odrl:lteq ;
        odrl:rightOperand "2022-12-31"^^xsd:date .
```

patient Data will be copied: yes/no yes

Fig. A1.6: Rule 2 represented in ODRL policy

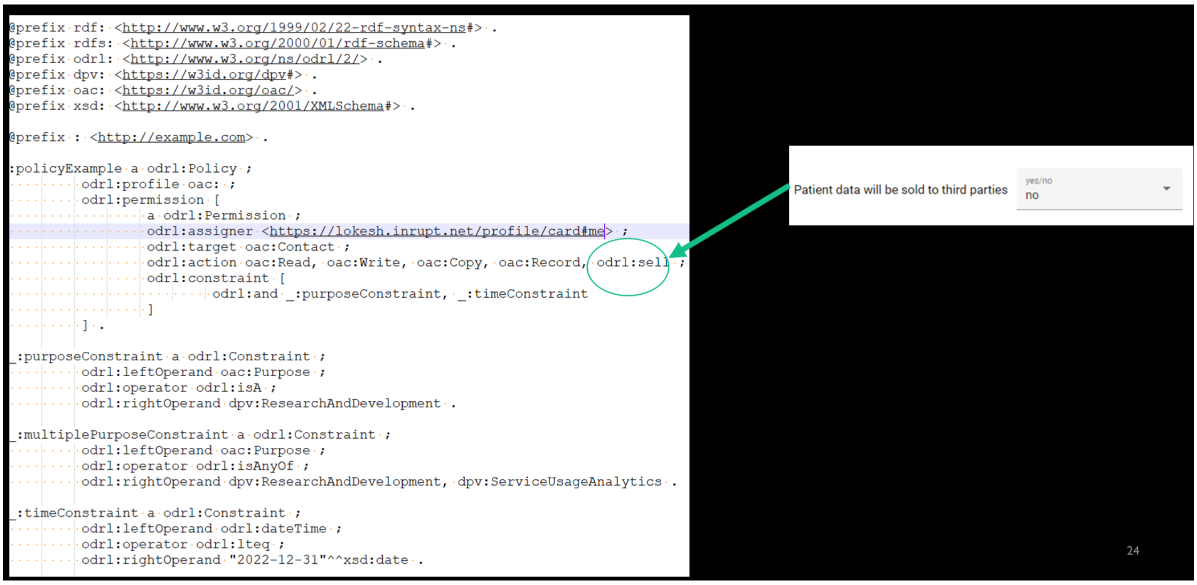


```
@prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> .
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#> .
@prefix odrl: <http://www.w3.org/ns/odrl/2/> .
@prefix dpv: <https://w3id.org/dpv#> .
@prefix oac: <https://w3id.org/oac/> .
@prefix xsd: <http://www.w3.org/2001/XMLSchema#> .

@prefix : <http://example.com> .

:policyExample a odrl:Policy ;
        odrl:profile oac: ;
        odrl:permission [
                a odrl:Permission ;
                odrl:assigner <https://lokesh.inrupt.net/profile/card#me> ;
                odrl:target oac:Contact ;
                odrl:action oac:Read, oac:Write, oac:Copy, oac:Record, odrl:sell ;
                odrl:constraint [
                        odrl:and _:purposeConstraint, _:timeConstraint
                ]
        ] .

_:purposeConstraint a odrl:Constraint ;
        odrl:leftOperand oac:Purpose ;
        odrl:operator odrl:isA ;
        odrl:rightOperand dpv:ResearchAndDevelopment .

_:multiplePurposeConstraint a odrl:Constraint ;
        odrl:leftOperand oac:Purpose ;
        odrl:operator odrl:isAnyOf ;
        odrl:rightOperand dpv:ResearchAndDevelopment, dpv:ServiceUsageAnalytics .

_:timeConstraint a odrl:Constraint ;
        odrl:leftOperand odrl:dateTime ;
        odrl:operator odrl:lteq ;
        odrl:rightOperand "2022-12-31"^^xsd:date .
```

history of data collected will be maintained

yes/no: no

Fig. A1.7: Rule 3 represented in ODRL policy

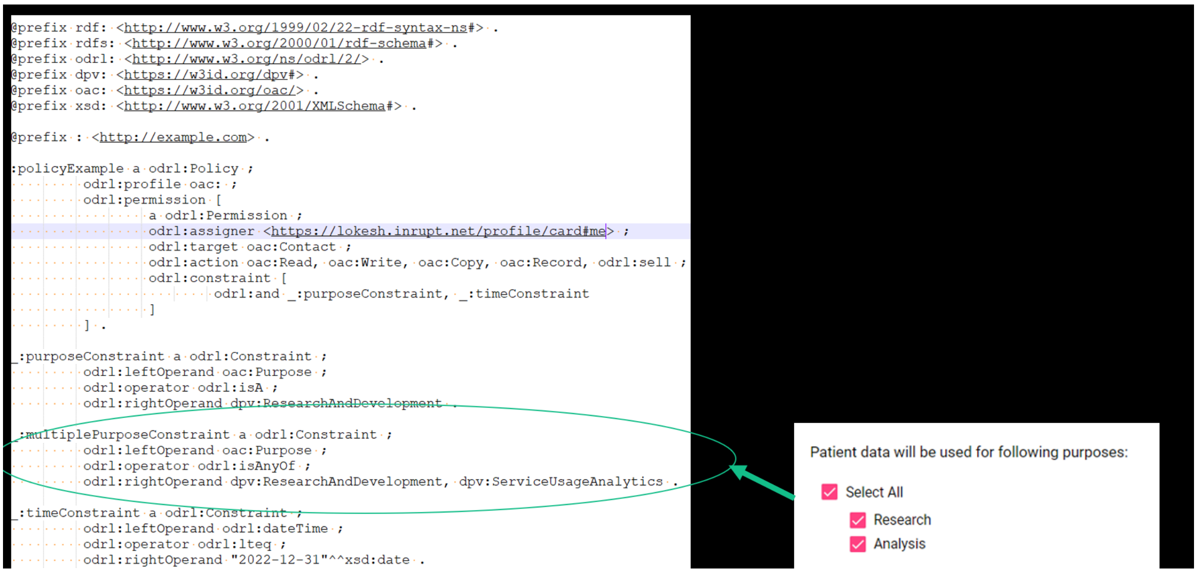


```
@prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> .
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#> .
@prefix odrl: <http://www.w3.org/ns/odrl/2/> .
@prefix dpv: <https://w3id.org/dpv#> .
@prefix oac: <https://w3id.org/oac/> .
@prefix xsd: <http://www.w3.org/2001/XMLSchema#> .

@prefix : <http://example.com> .

:policyExample a odrl:Policy ;
        odrl:profile oac: ;
        odrl:permission [
                a odrl:Permission ;
                odrl:assigner <https://lokesh.inrupt.net/profile/card#me> ;
                odrl:target oac:Contact ;
                odrl:action oac:Read, oac:Write, oac:Copy, oac:Record, odrl:sell ;
                odrl:constraint [
                        odrl:and _:purposeConstraint, _:timeConstraint
                ]
        ] .

_:purposeConstraint a odrl:Constraint ;
        odrl:leftOperand oac:Purpose ;
        odrl:operator odrl:isA ;
        odrl:rightOperand dpv:ResearchAndDevelopment .

_:multiplePurposeConstraint a odrl:Constraint ;
        odrl:leftOperand oac:Purpose ;
        odrl:operator odrl:isAnyOf ;
        odrl:rightOperand dpv:ResearchAndDevelopment, dpv:ServiceUsageAnalytics .

_:timeConstraint a odrl:Constraint ;
        odrl:leftOperand odrl:dateTime ;
        odrl:operator odrl:lteq ;
        odrl:rightOperand "2022-12-31"^^xsd:date .
```

Patient data will be sold to third parties

yes/no: no

Fig. A1.8: Rule 4 represented in ODRL policy



```
@prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> .
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#> .
@prefix odrl: <http://www.w3.org/ns/odrl/2/> .
@prefix dpv: <https://w3id.org/dpv#> .
@prefix oac: <https://w3id.org/oac/> .
@prefix xsd: <http://www.w3.org/2001/XMLSchema#> .

@prefix : <http://example.com> .

:policyExample a odrl:Policy ;
        odrl:profile oac: ;
        odrl:permission [
                a odrl:Permission ;
                odrl:assigner <https://lokesh.inrupt.net/profile/card#me> ;
                odrl:target oac:Contact ;
                odrl:action oac:Read, oac:Write, oac:Copy, oac:Record, odrl:sell ;
                odrl:constraint [
                        odrl:and _:purposeConstraint, _:timeConstraint
                ]
        ] .

_:purposeConstraint a odrl:Constraint ;
        odrl:leftOperand oac:Purpose ;
        odrl:operator odrl:isA ;
        odrl:rightOperand dpv:ResearchAndDevelopment .

_:multiplePurposeConstraint a odrl:Constraint ;
        odrl:leftOperand oac:Purpose ;
        odrl:operator odrl:isAnyOf ;
        odrl:rightOperand dpv:ResearchAndDevelopment, dpv:ServiceUsageAnalytics .

_:timeConstraint a odrl:Constraint ;
        odrl:leftOperand odrl:dateTime ;
        odrl:operator odrl:lteq ;
        odrl:rightOperand "2022-12-31"^^xsd:date .
```

Patient data will be used for following purposes:

☑ Select All

- ☑ Research
- ☑ Analysis

Fig. A1.9: Rule 5 represented in ODRL policy