**Abstract**

In Libya, Eritrean migrants frequently find themselves in a vacuum of knowledge. Due to their lack of contacts outside of Libya, they are forced to rely on smugglers for information, making it more difficult for them to flee human trafficking circumstances. The foundation of Social Linked Data (SOLID) is decentralised data management and storage. SOLID data pods, which are applicable to a variety of online applications, are used to store user data. This thesis introduces an information-sharing system that includes a SOLID-based platform for refugees to communicate their requirements, as well as a SPARQL-based Query Assistant for humanitarian associations to query and analyse data. SOLID data pods in Resource Description Framework (RDF) format are used to store refugee data, enabling queries that produce knowledge graphs and extract information. This platform serves as a tool for addressing the difficulties faced by Eritrean refugees.

# Contents

# List of Tables

## List of Figures

## List of Abbreviations

| | |
|---|---|
| **ICT** | Information and Communication Technology |
| **NGO** | Non-governmental Organisations |
| **GDPR** | General Data Protection Regulation |
| **W3C** | World Wide Web Consortium |
| **RDF** | Resource Description Framework |
| **SOLID** | Social Linked Data |
| **DGA** | Data Governance Act |
| **DA** | Data Act |
| **URI** | Universal Resource Identifiers |
| **URL** | Universal Resource Locators |
| **SPARQL** | SPARQL Protocol and RDF Query Language |
| **HTTP** | Hypertext Transfer Protocol |
| **LLM** | Large Language Model |
| **API** | Application Programming Interface |

# 1 Introduction

## 1.1 Problem Statement

Human trafficking, commonly referred to as 'modern-day slavery,' presents significant risks to global stability and human safety. It violates numerous international law standards and human rights protocols and is often conducted by criminals and members of well-organised crime networks around the world [50]. Human Trafficking for Ransom is traced back to the introduction of the mobile phone and the ubiquitous availability of mobile communication. Human Trafficking for Ransom was originally referred to as "Sinai Trafficking" by Van Reisen, Estefanos and Rijken [68], which was identified with refugees from Eritrea, which made up 95 percent of the hostages captured in Sinai [60] [70]. The situation of rampant smuggling and human trafficking can be traced back to the Eritrea-Ethiopia war of 1998-2000. Since this war, the Eritrean government has implemented a policy of mandatory national service [71]. The Eritrean population is drafted into the army without any assurance that their service will eventually conclude, leading many to flee to neighbouring countries and experience the isolation and hopelessness of living in exile. National Service, as it is called, is indefinite. Some have served for decades, yet have no prospect of release. Pay is derisory, conditions are grindingly tough, and there is routine abuse from officers. Women are in danger of sexual abuse and are frequently used as servants [53]. Many Eritreans cite their country's conscription policy for all adults between ages 18 and 50 as the main reason underpinning their decision to move; other key factors include poverty, a lack of opportunities and freedoms, and inadequate government services [38]

.

Moreover, information flow is strictly controlled in Eritrea. Eritreans find themselves in a closed society, where information is hard to get. There was no mobile telephone usage in Eritrea before 2003, and this increased to only 3.53 percent of the population who used mobile phones by 2010 — the lowest rate in the Horn of Africa. Also, Eritrea was the last country in Africa to establish local access to the Internet in 2000. In 2012, while the Internet usage rate for Africa was 15.6 percent (that is, its penetration as a percent of the total population of Africa), Eritrea's usage rate was 6.2 percent, much less than the 50 percent for Africa [12]. These factors contribute to the immigration situation of Eritreans.

While Eritrean refugees left their country in search of freedom, they are entrapped in a persistent cycle of human trafficking. They move between nations in the Horn of Africa and North Africa in their quest for safety, arriving first in Ethiopia and Sudan and then attempting or planning onward movements [45]. At the same time, crimes against humanity continue in Eritrea. Human trafficking is systematically conducted within the country, and the distinctions between human trafficking and smuggling are often unclear. Refugees suspect that traffickers operating inside Eritrea are linked to a larger network that functions outside the country, involving offenders along all pathways [69]. Many individuals who escape remain in the region but feel persistently at risk. Thousands of Eritrean refugees are sent back from Sudan and Egypt to Eritrea, where many vanish into national service camps, prisons, or worse outcomes. Their illegal status prevents them from accessing protection and makes them targets for exploitation. The policies of the EU are exacerbating this situation and trapping them in a human trafficking cycle [69].

The Mediterranean Sea ranks among the largest semi-enclosed seas. Migration within the Mediterranean, irregular or regular, has occurred for thousands of years [43]. It serves as a crucial entry point in the immigration path to Europe. The complex population movements, including refugees, asylum seekers, economic migrants and other migrants [11], have thus happened. Central, Eastern, and Western are three primary paths to Europe over the Mediterranean Sea. The Central Mediterranean route stretches from sub-Saharan Africa, mainly Libya, Tunisia, and Algeria, to Italy or Malta [6]. Libya's location has made it a gateway to further immigration routes. It plays a significant role as a transit nation for migrants heading to Europe due to its lengthy coastline of approximately 1,770 km to European destination States [24]. From the late 1990s, smugglers began using Libya as a launching pad to transport people from Libya by boat to Europe. As a result, Libya gradually emerged as a transit country and gateway to Europe [41]. According to data gathered by IOM's Displacement Tracking Matrix, between March and April 2020, some 600,000 refugees and migrants lived in Libya [42].

However, as a transition country, Libya is extremely dangerous for refugees. Migrants and refugees in Libya are considered unlawful due to Libyan law, which makes irregular entry, residence, and departure from the country a criminal offence. Human trafficking, abduction, detention, and extortion of migrants and refugees continued to flourish in Libya [31]. The risk of deportation makes them vulnerable to extortion (to avoid being sent back to Eritrea). Detainees were subjected regularly to torture, solitary confinement, held incommunicado, and denied adequate access to water, food, toilets, sanitation, light, exercise, medical care, legal counsel, and communication with family members [67]. They are looted, threatened, intimidated, violated, and held for ransom. Women routinely suffer sexual violence [71].

Criminal groups engaged in human trafficking for ransom in Libya thrive through Internet control and by establishing environments where they dominate all forms of communication [73]. Refugees in Libya do not have easy access to the Internet, and their voices are, therefore, often mediated by others [74]. Eritreans are caught in 'black holes' in the digital landscape – both in Eritrea, where Information and Communication Technology (ICT) and Internet connectivity are strictly controlled by the government, and when they flee, forced to depend on smugglers and traffickers [59]. Establishing digital black holes where individuals are excluded from the online world is crucial for upholding the control necessary for human trafficking for ransom to occur. Within these digital voids, restricted or absent Internet and digital access render those inside reliant on others for knowledge. ICTs are an essential component of the modus operandi of human trafficking for ransom: through mobile phones, ransoms are collected and mobile money transfers made [71]. Refugees struggle to create digital spaces, as in the holding camps, their access to smartphones is restricted. The victims of human trafficking find it difficult, if not impossible, to escape, even after paying large ransoms [23]. The effects of the extensive blockade were experienced by all, including non-governmental organisations (NGOs) and humanitarian aid groups. As stated in various NGO statements, the lack of access to transportation, communication, and financial services was said to have harmed the community by impeding the work of those agencies in distributing food and non-food items, as well as medical supplies, resulting in increased morbidity and mortality [51]

As a result, people outside remain unaware of the living situations of the refugees trapped in human-trafficking warehouses. The information about refugees' current dilemma is often unknown to their family members outside Libya and humanitarian organisations that provide assistance. The lack of adequate communication tools makes the challenges and struggles faced by the refugees unrecognised. Vulnerable refugees are left without the assistance they require due to this cycle of information scarcity [78] [77]. Refugees, therefore, need a way to let the outside world know that they need assistance. They frequently post about their living circumstances on Facebook and other social media platforms. It can be challenging to understand their current situation, though, if they have limited access to the internet. Social media gives refugees a platform for self-expression, but it also bears the potential for information misuse and the dissemination of false information, which could endanger their safety. Many refugees may want to stay anonymous out of concern for monitoring and possible retaliation, which makes it much more difficult for them to get help and correct information [69].

The security, privacy, and accessibility of refugees' personal information often present considerable challenges. The posting on public platforms presents security problems. The security issues pertain to the refugees, victims of human trafficking, and their families, who may be punished by association [39]. There are discrepancies between external information and the perceptions of refugees. The phones of migrants and refugees are taken from them, and they are dependent on the traffickers and those who work for them for information [23]. Refugees' limited understanding of how their data is collected, used, and protected may also contribute to widening the gap. Organisations that provide help often don't convey this information effectively. As a result, this gap can contribute to distrust among refugee groups, which makes it more complicated for organisations to provide assistance.

It's essential to manage refugees' personal data carefully as it contains sensitive information. The General Data Protection Regulation (GDPR) is the most prominent legal framework in this scenario. GDPR is an EU-wide legislation that replaced the Data Protection Acts 1988–2003. Several new provisions in GDPR were not previously in the Data Protection Acts 1988–2003. However, 80% of GDPR mirrors the provisions in the previous legislation. GDPR enhances the individual's data privacy and data rights and builds on the obligations and responsibilities of data controllers [58].

In Africa, the Malabo Convention regulates cybersecurity and personal data protection [7]. In June 2014, the African Union, Heads of States and Government adopted the Convention on Amendments to the Convention on the Statute of the African Court of Justice and Human Rights (known in short as the Malabo Convention) [4]. This Convention on the Establishment of a Legal Framework for Cyber-security and Personal Data Protection embodies the existing commitments of African Union Member States at sub-regional, regional and international levels to build the information society [7].

In our digital society, marginalised and vulnerable populations are unequally at risk of discrimination, surveillance, and a lack of representation from the collection, analysis, and usage of their data [13]. Technologies regarding secure, decentralised storage for individuals are emerging. The Semantic Web is a proposal to build an infrastructure of machine-readable semantics for the data on the Web. The World Wide Web Consortium (W3C) was created in October 1994 to lead the World Wide Web to its full potential by developing common protocols that promote its evolution and ensure its interoperability [63]. In 1998, the W3C recommended a metadata model and language to serve as the basis for such infrastructure, the RDF [10]. SOLID is based on RDF and Semantic Web technologies, and it achieves the goals of providing data independence and simple yet powerful data management mechanisms [61]. SOLID enables users to store their data in decentralised data pods, which function as a data storage warehouse. Users have control over the entry permissions, which can be withdrawn at any time. Such measures protect user data from unauthorised access or data breaches. By utilising SOLID, this research explores the use of a decentralised storage system in the context of refugee protection. Alongside, the RDF data format is used to ensure efficient data management for refugees. By leveraging SOLID, we aim to create a safe environment where refugees can store sensitive information, such as identification documents, medical records, and personal histories.

In conclusion, living conditions for Eritrean refugees in Libya are difficult. It's challenging for them to communicate their requests to people outside Libya, due to the lack of digital tools they could use. Thus, these vulnerable people are often caught up in a perilous cycle of human trafficking, where they can be exposed to violence and exploitation. Research on the sharing of sensitive personal data among Eritrean refugees in Libya is noticeably lacking. This study provides solutions based on SOLID technology to handle this critical and complex problem. Relevant rules and regulations will be considered in the research design to ensure compliance and ethical integrity.

## 1.2 Research Gap

We examined the difficulties that Eritrean refugees in Libya are facing and the anticipated developments they will experience. We must take a more effective and structured approach to sharing sensitive information about refugees while following regulatory frameworks. To provide timely assistance to refugees at risk, we also need to determine how to make the data more accessible. It is essential to do this while protecting privacy, given the sensitive nature of this personal data.

There is a significant gap in the assistance provided to refugees in Libya. Essential technologies that facilitate humanitarian support and information dissemination are lacking. Furthermore, data security cannot be guaranteed, and the role of the GDPR and the Malabo Convention [7] in safeguarding data privacy is absent. Research aimed at adapting these platforms to enhance data security, privacy, and accessibility remains incomplete.

SOLID data pods have been introduced to facilitate secure data sharing. SOLID was initiated in 2016 and is led by WWW-inventor Tim Berners-Lee [49]. This research will examine how the use of the SOLID tool can address the identified issues in refugee assistance while adhering to the relevant regulatory frameworks. By doing so, we aim to propose an information exchange system that ensures data privacy and security.

Few studies have been conducted on the use of SOLID data pods to manage and share refugees' personal information. Therefore, our goal is to assess the feasibility of this specific application and propose an information exchange framework that supports refugees in Libya using innovative methods.

## 1.3 Research Objectives

The primary goal of this project is to propose a system design for a comprehensive information broadcasting platform, developed within a SOLID framework, ensuring that Eritrean refugees in Libya have a secure and reliable method for exchanging personal information.

In order to achieve this goal, multiple sub-objectives were recognised:

1. Analyse refugees' current data-sharing format and the danger they face.
   - The first step is to identify the current problems that refugees face, as reported by refugees and those working in refugee protection.
   - It is crucial to determine how refugees currently share and report their situations and how they communicate through technical tools.

2. Understand the requirements and architecture under the safety protection and regulatory framework.
   - The first step involves reviewing GDPR and the Malibu Convention to understand current data protection law.
   - The next step is to hold a co-creation session with refugees and NGO workers to understand the actual needs of users and ensure the system applies to real situations. Establish requirements and specifications of the design to be created.

3. Design an accessible SOLID system that improves communication with refugees.
   - We aim to use innovative tools and information technology to ensure that refugee data is stored safely and shared efficiently.

4. Assess the capabilities and function of the SOLID system.
   - In this section, we assess and validate the practicality of the proposed technical architecture, ensuring its effectiveness and reliability in real-world applications.

## 1.4 Research Questions

Therefore, we ask: How can implementing SOLID principles in the information broadcast platform for Eritrean refugees in Libya contribute to building an infrastructure that preserves privacy and facilitates communication?

The questions that we use to answer the main research question ultimately are as follows:

1. What is the current information exchange situation of refugees?
   - What actions are currently lacking in humanitarian assistance and information sharing for Eritrean refugees in Libya?
   - What are the restrictions with regard to the availability of such information?

2. What are the key features and functionalities required to improve the accessibility of this SOLID application?
   - What types of personal information do NGOs consider most critical for providing care to refugees, and what information should be accessible to them?
   – How should a refugee information exchange system, designed according to SOLID guidelines and principles, be constructed to enable NGO workers caring for Eritrean refugees in Libya to share personal information while ensuring privacy?

3. How can a safe system be designed to broadcast information among refugees effectively?
   - What appropriate tools should we utilise to ensure efficiency, scalability, and ease of use?
   - How could we receive and store sensitive data within a SOLID architecture?

4. What are the system's functionalities, and how do they align with its intended purpose?
   - What is the evaluation of the practicality of the suggested technical framework?

## 1.5 Hypothesis

Applying SOLID principles in the refugee protection field will create an information infrastructure that guarantees data provenance and improves information communication. Additionally, this approach will uphold data safety and facilitate access control under clearly defined conditions, helping to protect the privacy of Eritrean refugees in Libya and to retain control over personal information at the source.

## 1.6 Conceptual Framework

### 1.6.1 Information Black Hole

'Black holes' in the digital landscape are places or situations where connectivity is unavailable or deliberately denied [23]. Black holes are proof of the inability of the architecture and digital infrastructure of the Internet to facilitate African voices on their own terms [72]. Libya can be described as a black hole in the information landscape, especially in places that are under the control of fragmented militias. In 2018, Freedom House (2018) analysed Internet freedom in Libya and noted that the country suffers from both physical obstacles (such as power outages) and restrictions on freedom of the press. There is limited access to the Internet, and access is controlled [48]. The human traffickers and those who work for them control what information is shared, playing a strict gatekeeping role with the flow of information [73]. Unequal access to digital technologies has contributed to the continuation of this situation. Blocking those most vulnerable from accessing the Internet and controlling their communication gives power to the trafficking networks [69]. The refugees are kept in black holes in the digital landscape, unable to receive or disseminate information.

In the digital era, the amount of access to digital infrastructure is an aspect of power that can be exercised. If information access is suppressed or disabled, this creates social dependencies [33]. Refugees trapped in the human trafficking cycle often lack access to information, being isolated from the outside world. The communication barriers create an environment where refugees are excluded from accessing essential support resources. Thus, refugees controlled by human traffickers often have difficulties accessing available assistance, making the situation worse. Moreover, the management of their data is concerning. The information collected from these individuals is stored and shared in an insecure manner, and has the potential for data breaches. This lack of transparency raises serious ethical questions about privacy and consent.

### 1.6.2 Resource Description Framework

The existing World Wide Web mainly promotes human navigation and searches for textual data. With the growing volume of available content, this approach has become increasingly insufficient. What is needed instead is a framework that enables integrated and consistent access to information sources and services, along with intelligent applications for processing information on the Web. This kind of framework necessitates standardised methods for data interchange and the management of various data semantics. The RDF represents progress toward this goal. The RDF model presents data in the form of triples. Each triple comprises the resource being described (referred to as the subject), a property of that resource (the predicate), and the corresponding value (the object) [36].

RDF represents the main ingredient and data representation format for Linked Data and the Semantic Web. It supports a generic graph-based data model and data representation format for describing things, including their relationships with other things [79]. RDF facilitates interoperation because it provides a data model that can be extended to address sophisticated ontology representation techniques [25]. It supports fast integration of data sources by bridging semantic differences. It is often used (and was initially designed) for representing metadata about other Web resources [26].

### 1.6.3 Social Linked Data

SOLID is a web-based, decentralised data storage solution that enables users to own and control their data. SOLID is based on RDF and Semantic Web technologies, and it achieves the goals of providing data independence and simple yet powerful data management mechanisms [61]. In SOLID, individuals keep their information in an online storage area known as a personal online datastore (pod). Pods are storage services accessible via the web. They can be hosted on personal servers that users manage themselves or on public servers provided by pod providers similar to existing cloud storage services. Users can have multiple pods if they wish. A user can select from various pod providers, as SOLID applications are compatible with any pod server, irrespective of its location or the services offered by the provider. Different pod providers can offer different degrees of privacy, reliability (e.g., availability or latency guarantees), or legal protection (e.g., the legal framework specific to the country where the pod is hosted) [61].

In SOLID, applications use authentication protocols to discover the user's identity and profile data, as well as relevant links that point to the user's pod and application data. Decentralised authentication, a global ID space, and global single sign-on are a critical part of the Solid ecosystem [61]. Based on the separation of data and applications, the vision defines an ecosystem that facilitates the integration of data in different applications, while keeping people in direct control of their data [27].

## 1.7 Ethical and Legal Considerations

### 1.7.1 Laws and regulations

Data management has become one of the prime factors of concern in all fields of contemporary research [54]. To understand how data can be processed, it is essential to identify applicable principles of data governance and the regulatory frameworks.

**Data Governance**
Data governance is an emerging subject in the field of information systems. In recent years, the volume of data used within organisations has increased dramatically [8]. Data governance refers to establishing policies concerning data acquisition, management, and storage. Its significance continues to grow as organisations face new data security laws. The purpose of data governance is to increase the value of data and minimise data-related cost and risk [5]. For example, data governance encourages compliance with regulations like the European Union's GDPR [1] and Africa's Malabo Convention [7].

**General Data Protection Regulation**
Adopted in 2016, the GDPR came into force in May 2018. It provides for numerous new and intensified data protection obligations, as well as a significant increase in fines (up to 20 million euros) [75]. The GDPR expands the scope of data protection so that it applies to anyone or any organisation that collects and processes information related to EU citizens, no matter where they are based or where the data is stored [66]. EU's GDPR also has implications for African states [80]. GDPR demands significant data protection safeguards and poses both new challenges and potential opportunities to organisations around the world [47].

The data subject has the right to request transparent information. As stated in GDPR Article 12 (1), the controller shall take appropriate measures to provide any information and any communication relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing or by other means, including, where appropriate, electronic means. When requested by the data subject, the information may be provided orally [1].

In GDPR Article 13 (1), it points out that when personal data is collected from the data subject, the collector should provide the following information [1]:

1. the identity and the contact details of the controller and, where applicable, of the controller's representative;

2. the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing;

The data subject has the right to request confirmation from the controller regarding whether personal data related to them is being processed, and, if so, access to that personal data along with the following details, as mentioned in GDPR Article 15 (1): the purposes of the processing and the categories of personal data concerned [1].

As outlined in GDPR Article 25 (2), the data controller shall implement appropriate technical and organisational measures to ensure that, by default, only personal data necessary for each specific processing purpose is processed [1].

**Malabo Convention**

In June 2014 the Assembly of the African Union adopted the Malabo Protocol (also known as Malabo Convention) which in its Annex includes amendments to the Statute of the African Court of Justice and Human and Peoples' Rights empowering the Court with international criminal jurisdiction [2]. The Convention entered into force in June 2023 after receiving its 15th ratification [80]. The Malabo Convention established a regulatory framework on cybersecurity and personal data protection. It takes into account the requirements of respect for the rights of citizens, guaranteed under the fundamental texts of domestic law and protected by international human rights Conventions and Treaties, particularly the African Charter on Human and Peoples' Rights [7].

The Malabo Convention defines personal data, which means any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity [7]. The definition of sensitive data is also stated: sensitive data means all personal data relating to religious, philosophical, political and trade-union opinions and activities, as well as to sex life or race, health, social measures, legal proceedings and penal or administrative sanctions [7].

### 1.7.2 Ethical Considerations

In the problem exploration part, it's essential to communicate the rights of both the researcher and the participants before taking interviews. Before each interview, the objectives and significance of the research were explained to the participants. Interviewees were aware that the meeting would be recorded and that their involvement was voluntary. Additionally, there are key rights to address regarding the procedures after the interview. Once the research has concluded, the recordings will be erased. Moreover, it has been agreed that the interviewees will not be identified by their names in the final thesis.

## 1.8 Relevance

### 1.8.1 Social Relevance

The social relevance in academic research emphasises the ability to contribute to solving societal problems, meeting societal needs, and positively impacting society. It focuses on the importance of research in addressing communities' complex issues. Regarding this, the proposed study centres on the requirements of Eritrean refugees in Libya, a nation severely impacted by the current conflict. The study will aid in the improvement of humanitarian organisations that provide support to refugees by examining the complex challenges they face.

Additionally, this study has the potential to provide information about the topic of refugee protection in Libya, especially in light of the growing concern about human trafficking. The results could inform future research and policy actions aimed at enhancing the protection of vulnerable populations in the area by addressing the interconnection of these concerns. Ultimately, the study seeks to address critical knowledge gaps and inspire practical solutions that promote the rights and welfare of refugees, thereby supporting the broader humanitarian effort in Libya.

### 1.8.2 Academic Relevance

On the other hand, academic relevance refers to the importance and innovativeness of the research topic within the educational field. It emphasises the potential impact of the research on existing knowledge and practices, while aligning with current trends and challenges in academic research. This relevance is demonstrated through the topic's ability to address present issues, fill gaps in the literature, or introduce novel methodologies that enhance outcomes.

The academic relevance of this thesis stems from its aim to utilise SOLID in developing an architecture which serves as a portal for exchanging sensitive personal data of Eritrean refugees in Libya who require humanitarian aid. Furthermore, there is a lack of academic resources focused on designing an architecture that complies with regulatory standards while addressing the needs of the intended users. This thesis has the potential to serve as a groundwork for subsequent academic inquiries.

## 1.9 Location and Timeline

This thesis has been conducted for the master's program in Computer Science at Leiden University. We worked with refugee communities from Eritrea in the Netherlands and Kenya. The research aims to explore how to securely exchange personal information for these vulnerable individuals, who have limited access to the Internet and technology, making it difficult for them to receive humanitarian assistance from NGOs.

The methodology employed in this study is the case study research method, which involves gathering insights from social workers in the refugee protection sector. Based on the findings, a personal data exchange framework is proposed. A proof of concept will be conducted to validate the effectiveness of this framework.

This research is being carried out from September 2024 until July 2025. Figure 1 shows the project timeline.


Figure 1: Thesis timeline.

## 1.10 Research Approach

We first consider the various paradigms that exist within the academic sector to define our research methodology. By utilising these paradigms, the research can be conducted in an organised way. To fully understand user needs and preferences, this study combines a range of qualitative research techniques, including interactive co-creation workshops and in-depth interviews. We aim to gather insights from participants in these sessions. Furthermore, we combine technical concepts with prototyping methods to create innovative solutions tailored to the needs that have been identified. Through iterative design and testing, we work to improve these solutions and make sure they are both useful and user-centred.

There are two categories of research: qualitative and quantitative. Quantitative data is numerical information about the world, presented in the form of numbers. In contrast, qualitative data can therefore be defined as empirical information about the world, not in the form of numbers [56]. Qualitative methods primarily focus on non-numerical data, including videos, transcripts, and images. These types of data often provide a rich array of descriptive and explanatory information. In qualitative research, data is typically gathered through open-ended questions, which enable participants to express their opinions and feelings freely. Qualitative approaches to data collection and analysis are powerful tools, which can enrich the study of social networks in substantial ways [37]. Engineering solutions refer to utilising engineering concepts and techniques to address real-world challenges. This method is particularly prevalent in technical disciplines such as engineering, computer science, and physics. The engineering solutions emphasise practicality, innovation, and a systematic process, aiming to develop systems that address specific issues. By combining qualitative methods with engineering solutions, a more comprehensive research design is created, providing a more effective solution to the problem.

## 1.11 Research Design

The research design used a mixed method to ensure a comprehensive problem analysis. Both qualitative and engineering methods were deployed to explore the research questions thoroughly. Qualitative data was collected through in-depth interviews and a co-creation session, providing rich insights into participants' experiences and perspectives. The engineering part offered a technical solution to the problem. By combining these methods, the research aimed to achieve a holistic understanding of the current topic.

1. *Interviews:* A series of in-depth interviews will be undertaken with refugees, NGO workers and researchers to gain comprehensive insights regarding refugees' problems. For example, we aimed to understand the existing communication barriers and required support. The interviews enable us to gain a better understanding of their perspectives. The diverse group of interviewees also offers a wide range of views related to the problems existing in the refugee groups.

   The backgrounds and language proficiency of the interviewees may vary, so they may have different interpretations of the same question. This variability requires a flexible approach during the interviews; being adaptable will allow us to navigate these diverse answers effectively. Open-ended interview questions will help us foster an atmosphere of trust and openness and encourage interviewees to share their views freely. In this way, we can build a deeper connection with participants and gain meaningful insights about their experiences.

2. *Co-creation:* After the interviews, a co-creation session will be held to delve deeper into the requirements and expectations of our users, specifically refugees. This co-creation will engage people from different fields, including data stewards, researchers and NGO workers. It's a collaborative approach to discuss the system functions that will address the problem efficiently. Each participant is encouraged to share their insights and experiences related to the current problem. This approach will provide useful ideas for the system design, making sure the product is tailored to the actual needs of refugees.

This collaborative effort enables participants to translate their insights into functional requirements, leading to a deep understanding of system functionalities. Requirements from the users' perspective will result in a solution that can effectively reflect the needs of the refugee communities.

3. *Engineering:* After identifying the problems and key requirements from interviews and the co-creation, we integrate engineering solutions to address the needs of refugees and establish a comprehensive support system. This process will utilise a range of programming languages and technical tools in computer science to build the system. The focus is on translating the identified requirements and specifications into a technical design that can be tested. This approach will prioritise adaptability, enabling us to refine our system based on user feedback.

4. *Assessment:* To test the system's capabilities and reveal potential enhancements, comprehensive tests of the final product will be conducted using mock data. Users will evaluate the system and provide feedback based on the testing experience. It is crucial to systematically identify the product's strengths, weaknesses, and improvement in future development. This process will facilitate a thorough evaluation of the engineering process and foster continuous improvement.

### 1.12 Thesis Outline

This thesis comprises the following sections: Chapter 2 will explore the theoretical framework in detail. Chapter 3 will describe the research methodology used to tackle the various research questions presented. Chapter 4 will showcase the research findings. Subsequently, Chapter 5 will evaluate and interpret the results, noting any limitations and proposing future research directions in the discussion section. Lastly, Chapter 6 will summarise the conclusions drawn from the research findings.

# 2 Theoretical Framework

It's vital to establish a theoretical foundation for our research before presenting the findings. This chapter focuses on exploring concepts relevant to system implementation. We will investigate the details of decentralised technology, which is crucial in offering technical solutions. The goal is to provide a thorough understanding of the theoretical foundations that will guide the implementation of the system.

## 2.1 Black Holes in the Digital Landscape

Nowadays, Information and Communication Technologies (ICTs) have spread extensively in everyday life in an unprecedented way. With the immersive invasion of the internet, smartphones' applications, and digital social networking, people become more socially connected through virtual spaces instead of meeting in physical public spaces [3]. The digital divide is a phenomenon linked not only to the topic of access to the Internet, but also to the topic of usage and usage benefits. It refers to unequal patterns of material access to, usage capabilities of, and benefits from computer-based information and communication technologies caused by certain stratification processes that produce classes of winners and losers of the information society, and participation in institutions governing ICTs and society [32]. This establishes a new social framework where the privileged benefit while others find themselves trapped in the 'black holes' of informational capitalism. Such black holes are not just caused by a lack of access to devices or connectivity, although this can play a role, but access can also be deliberately limited or denied [69].

Access to and use of mobile phones and the internet are among the most critical indicators of contemporary ICT development. ICT use can affect why, how and the scale on which people move. Mobile phones facilitate immediate communication and connectivity, enabling users to interact socially, access information, and utilise various services. Similarly, internet access effectively bridges geographical gaps. The most recent datasets of the World Bank (2020) and the International Telecommunication Union (ITU) (2018) indicate that globally, there are on average 106 mobile phone subscriptions per 100 people. Eritrea has only 20 subscribers per 100 people, followed by South Sudan (33 per 100 people) and Ethiopia (37 per 100 people) [22]. Without available communication tools, refugees may rely on others for access to the Internet, and they are defined as information gatekeepers, who collect information regarding the surroundings, filter it, translate it into the group's language and distribute it for use within the group [19]. The flow of information is tightly controlled by various gatekeepers, often referred to as smugglers. Smugglers in Libya are gatekeepers for refugees who have been captured by the human trafficking networks going through Libya. This makes it extremely difficult for Eritrean refugees to obtain information and communicate their needs for help, effectively trapping them in an information black hole within the human trafficking network.

## 2.2 Decentralised Web and Data Sovereignty

### 2.2.1 Decentralisation

Social networking platforms have become increasingly popular in recent years due to the ease and speed with which they allow individuals to connect with one another and share a variety of information. However, the control, governance, and management of the web have become increasingly centralised, resulting in security, privacy, and censorship concerns [44]. Centralised paradigms limit users' mobility and, ultimately, their chances of establishing new relationships and benefiting from diverse networking services [18]. The decentralised web has emerged to solve these issues. These offer alternatives to traditional social networks like Twitter, YouTube, and Facebook, by enabling the operation of web infrastructure and services without centralised ownership or control [57].

Decentralisation is often used as a general term for describing network architectures that more precisely span from decentralised to distributed [17]. Figure 2 shows one widely referenced classification of network topologies, distinguishing between centralised, decentralised, and distributed networks. A centralised network consists of a primary node or a group of closely linked nodes that connect to all other nodes in the system, with all these different nodes only linked to this one main node. As a result, if the central node fails or is destroyed, it cuts off all nodes from the network and stops them from communicating with one another. On the other side, in a decentralised network, a structure of nodes is arranged in a hierarchy, where the nodes at the lower tier essentially form a small star network that links them to a node located one level above in the hierarchy. These nodes, in turn, form part of another star network that connects them to the next higher-level node in the hierarchy. Failure of a few nodes in a decentralised network still leaves several connected components of nodes that can communicate with each other (but not with nodes in a different component) [17]. Finally, distributed networks consist of nodes with approximately equal connections to others. Even if several nodes fail, the network remains connected, enabling all nodes to communicate with one another.

In a decentralised web, data was distributed across networks, and no single entity owned the information. The goal was to extend the Internet to more people, use it, apply it, and give it human meaning and impact for social and environmental benefit [64]. The decentralised web improves data privacy while enabling interoperability across different platforms. Individuals have stronger control over their data in a decentralised web, as the data is stored in a distributed manner across multiple nodes instead of a centralised server. This structure reduces the likelihood of large-scale data breaches, which are more common when sensitive information is stored in a single location.

Moreover, decentralised web technologies promote interoperability among diverse applications and platforms. Unlike the centralised web, each platform typically has its own ecosystem where data silos often exist. Decentralisation allows for seamless interaction and integration of services. Using protocols, developers can collaborate on creating interoperable applications that provide users with a cohesive experience. This interoperability fosters a more connected and user-friendly digital landscape. Overall, the decentralised web reshapes how people engage with technology, prioritising privacy, security, and joint creation.

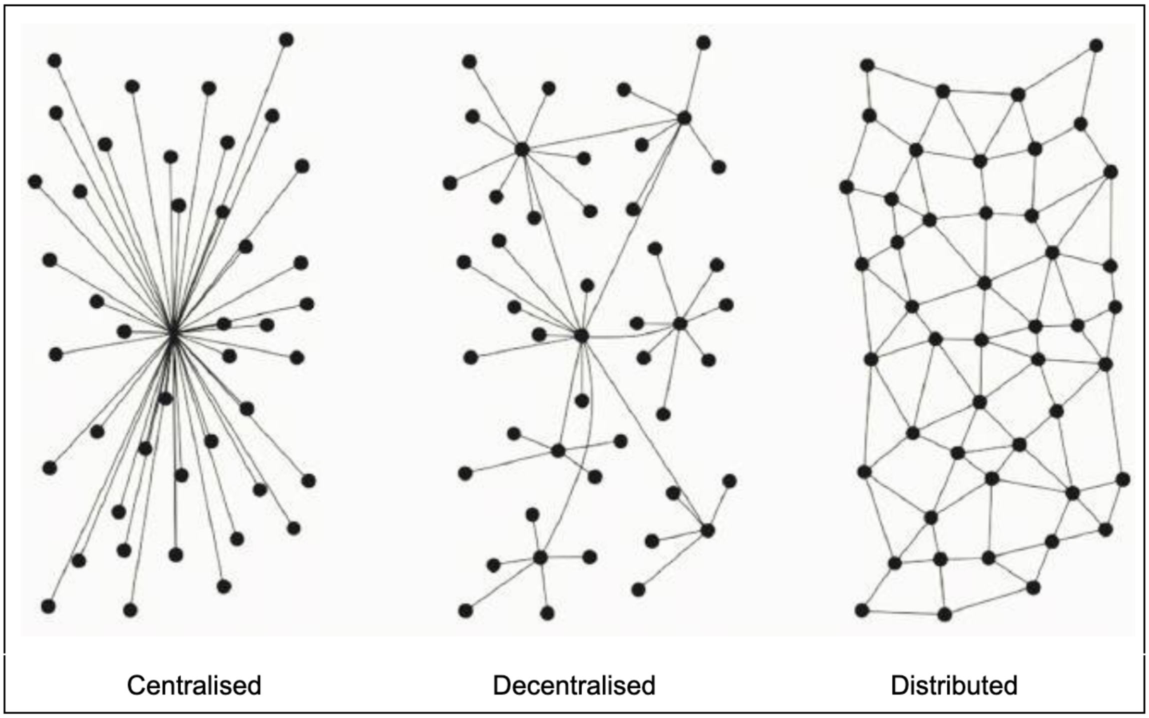



Figure 2: Baran's typology of communication networks. Source: Baran, 1964, p.2.

### 2.2.2 Data Sovereignty

Recent years have seen an emergence of the notion of data sovereignty in debates on the development, implementation, and adjustment of new data-driven technologies and their infrastructures [40]. The term 'data sovereignty' is a uniquely twenty-first-century expression that arises directly from the explosive growth of information associated with the internet and the spread of mobile phone technology. Data sovereignty refers to managing information in a manner consistent with the laws, practices, and customs of the nation-state in which it is located [65]. It guarantees that organisations, governments, and individuals maintain authority over their data. This authority enables them to determine their own choices regarding the collection, storage, sharing, and usage of their data by others. Data sovereignty constitutes a key piece in building safe environments where data providers and consumers overcome trust issues while sharing data. Legislations derived from the European Strategy for Data, such as the Data Governance Act (DGA) or the Data Act (DA), as well as the GDPR that came into force in 2016, regulate the data protection of different actors [76]. Their emphasis on individual control and organisational accountability constitutes a new paradigm that requires changes in the way organisations manage personal data [46].

However, the current movement toward open data and open science does not fully engage with the rights and interests of indigenous peoples. Existing principles within the open data movement (e.g., FAIR: findable, accessible, interoperable, reusable) primarily focus on characteristics of data that facilitate increased data sharing among entities, while ignoring power differentials and historical contexts. The emphasis on greater data sharing alone creates a tension for indigenous people who are also asserting greater control over the application and use of indigenous data and indigenous Knowledge for collective benefit [34]. Indigenous Peoples' rights and wellbeing should be the focus across data ecosystems and throughout data lifecycles to minimise harm, maximise benefits, promote justice, and enable future use [21].

This includes the right to create value from indigenous data in ways that are grounded in indigenous world-views and realise opportunities within the knowledge economy. The CARE Principles for Indigenous Data Governance (Collective Benefit, Authority to Control, Responsibility and Ethics) are people and purpose-oriented, reflecting the crucial role of data in advancing indigenous innovation and self-determination [34]. The CARE Principles are designed to complement the FAIR Principles and guide the inclusion of Indigenous Peoples in data processes that strengthen Indigenous control for improved discovery, access, use, reuse, and attribution in contemporary data landscapes [21].

First Nations are indigenous peoples. Every First Nation has the inherent right to make informed decisions about how its information is shared. Historically, research and data collection practices have not always been beneficial to or respectful of First Nations' rights or interests. The OCAP principles establish how First Nations' data, information, and cultural knowledge should be collected, accessed, used, and shared. OCAP stands for: Ownership, Control, Access, and Possession [30].

The OCAP and CARE principles developed by indigenous residents integrate the differences in social levels. They offer a data management model rooted in communities that can inform refugee data rights in a practical way.

### 2.3 Semantic Web

Most web content is suitable for human consumption. Even web content that is generated automatically from databases is usually presented without the original structural information found in databases. An alternative approach is to represent web content in a form that is more easily machine-processable and utilise intelligent techniques to leverage these representations. We refer to this plan of revolutionising the Web as the Semantic Web initiative [9]. The Semantic Web was propagated by the W3C, an international standardisation body for the Web. The driving force behind the Semantic Web initiative was Tim Berners-Lee, the inventor of the World Wide Web in the late 1980s. He expects from this initiative the realisation of his original vision of the Web, a vision where the meaning of information played a far more critical role than it does in today's web [9].

The Semantic Web is not an entirely different web; rather, it is an enhancement of the existing one, allowing information to be assigned clear meanings, which facilitates improved collaboration between computers and humans. It was achieved through incremental changes, by incorporating machine-readable descriptions into the data and documents already on the Web [20]. While a web browser navigates along links between documents, a semantic web browser navigates along relationships (predicates) in a web of concepts [15]. With the Semantic Web, web pages will include annotations (either embedded within the pages or located externally) that formally summarise the information within. Applications of the Semantic Web will utilise that knowledge to automate web tasks that currently require notable user involvement.

Interpersonal communication has been transformed by the World Wide Web. It functions as a key component in transforming societies into a knowledgeable community. The connections built by the web have rebuilt social interactions and enhanced the spreading of knowledge, ultimately contributing to a more joint society.

### 2.3.1 Resource Description Framework

On the Semantic Web, anyone will be able to annotate web pages, and these annotations will not be limited to a fixed vocabulary [62]. This requirement led to the definition of RDF, a standard recommendation for representing knowledge on the Semantic Web. It provides developers with robust tools for formulating statements and linking them to extract meaning. RDF presents a more robust framework for data representation compared to XML or relational databases.

Within the RDF specification, an RDF triple consistently documents these three pieces of information, ideally allowing both human and machine consumption of the same data [55]. An RDF model consists of a collection of triples, where each triple includes a subject (the resource that is being described, such as a webpage), a predicate that identifies the attribute defined for that resource, and an object representing the specific value of the predicate for the given subject. For example, one way to simplify is by using the following to denote a triple:

$$\{\text{subject, predicate, object}\}$$

Following this, an example of an RDF triple could be:

{http://burningbird.net/articles/monsters3.htm, title, ”Architeuthis Dux” [55]}

In this triple, the URI, *http://burningbird.net/articles/monsters3.htm* represents the subject, *title* is the predicate, and *Architeuthis Dux* is the object. This indicates that the title of the URI is *Architeuthis Dux*. Every RDF triple represents a unique and complete fact.

Resources in RDF are identified by URIs (Universal Resource Identifiers). A URI can be further classified as a locator, a name, or both. URLs (Uniform Resource Locators) are the most common type of URIs. It refers to the subset of URIs that, in addition to identifying a resource, provide a means of locating the resource by describing its primary access mechanism (e.g., its network ”location”) [16]. A locator helps you find something, like a web page, and an identifier identifies something [29]. The subject and predicate of an RDF triple are URIs. Anyone can identify new resources to describe and new properties of resources simply by assigning a new URI to them [62].

The assertions within various RDF files can be effectively combined, resulting in a more comprehensive dataset than any individual file could provide. Each RDF triple, composed of a subject, predicate, and object, facilitates a structured representation of data, enabling both human understanding and machine processing. Although each RDF triple can be combined with other RDF triples, it retains its unique significance, regardless of how complex the model it belongs to may be. This standardised approach allows for consistent interpretation of relationships and meanings across diverse datasets, making it easier to perform queries, integrate information from multiple sources, and derive insights that would otherwise remain obscured when the data is analysed in isolation. RDF supports flexible and powerful query structures, and developers have created various tools for working with RDF [55].

### 2.3.2 SPARQL Protocol and RDF Query Language

The SPARQL Protocol and RDF Query Language (SPARQL) is the W3C candidate recommendation query language for RDF. It is a graph-matching query language designed for retrieving RDF data, a standard model for representing information commonly used in the Semantic Web. The Protocol part of SPARQL's name refers to the rules for how a client program and a SPARQL processing server exchange SPARQL queries and results. These rules are specified separately from the query specification document and are mostly an issue for SPARQL processor developers [29]. Using SPARQL, users can request and manage RDF data in a declarative format. With a data source, a query is created by comparing it with this data source. Results from this comparison are then processed to get the answer. The queried data source may contain diverse sources.

A SPARQL query is made up of three elements. The pattern matching section highlights several intriguing aspects of graph pattern matching, including optional components and the choice of data sources to which a pattern can be applied. The solution modifiers come into play after the pattern's output has been generated (presented as a table of variable values), enabling adjustments to these values through the use of standard operations. Finally, the output of a SPARQL query can be of different types: yes/no queries, selections of values of the variables which match the patterns, construction of new triples from these values, and descriptions of resources [52].

SPARQL fosters querying across different databases. This ability is particularly useful when data is spread across multiple locations. After querying the external database, the results are returned to the local database. Information is then filtered and refined to finalise the query, which streamlines data integration. It serves as a powerful tool for minimising complexity while improving interoperability across different datasets.

### 2.3.3 Linked Data Principles

The Semantic Web is not exclusively focused on putting data online; it aims to create links that allow people and machines to navigate the extensive information web. With Linked Data, having access to part of the information enables one to uncover more relevant data. Linked data serves as a tool for interconnecting structured data on the internet. Tim Berners-Lee introduced these practices in his architectural note, ”Linked Data”, and has become recognised as the principles of Linked Data [14]. The following are these principles:

- Use URIs as names for things.
- Use HTTP URIs so that people can look up those names.
- When someone looks up a URI, provide useful information using RDF, SPARQL standards.
- Include links to other URIs, so that they can discover more things [14].

The first principle, ”use URIs as names”, advocates using URI references to identify, not just Web documents and digital content, but also real-world objects and abstract concepts [35]. This includes items such as individuals, locations, and vehicles, as well as more abstract entities. This principle can be interpreted as broadening the Web’s reach from merely online resources to include any object in the real world. The Hypertext Transfer Protocol (HTTP) is the web’s universal access mechanism. In the classic web, HTTP URIs are used to combine globally unique identification with a simple, well-understood retrieval mechanism [35]. The second principle of Linked Data emphasises the importance of using HTTP URLs to specify both objects and abstract concepts, allowing these URIs to be accessed via the HTTP protocol to obtain a description of the specified object or concept [35]. To allow various applications to handle web content effectively, it is crucial to establish standardised content formats. Consequently, the third principle of Linked Data promotes the adoption of a universal data model for disseminating structured data on the web. The fourth principle of Linked Data emphasises the importance of using hyperlinks to link not just web documents but also various entities [35]. For instance, a hyperlink can be established between a person and a location or between a location and a business. Unlike traditional web links, which are mostly untyped, hyperlinks in a Linked Data framework have specific types that define the relationships between the entities.

The basic idea of Linked Data is to apply the general architecture of the World Wide Web to the task of sharing structured data on a global scale. The development and use of standards enables the web to transcend different technical architectures. In summary, the Linked Data principles lay the foundations for extending the web with a global data space based on the same architectural principles as the classic document web [35].

### 2.3.4 SOLID

SOLID is a decentralised data storage solution that operates on the web, allowing users to possess and manage their own data. SOLID utilises Semantic Web technologies to separate user data from applications, making it easy for users to switch between applications that use the same data and between storage providers that host the data [61]. Figure 3 shows the architecture of SOLID. In the SOLID framework, users are required to register with an identity provider, typically their pod provider. The identity provider maintains the user’s WebID profile document, which is linked to a cryptographic key.

The main focus of SOLID is to facilitate information sharing while ensuring data privacy and security. Personal data is stored in decentralised data pods, also known as data storage warehouses. Authenticated applications have access to the data, provided that the user has granted permission to the application. It’s possible to store personal data across multiple pods, which keep different types of information. Users can

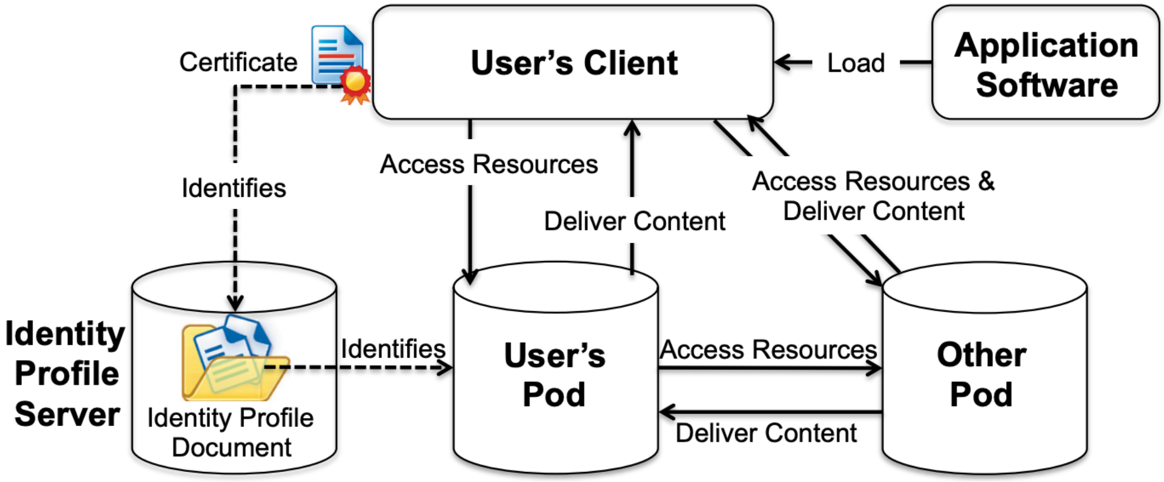



Figure 3: SOLID architecture [61]. The user manages their identity through an RDF profile document, typically kept on a pod server. The user accesses a SOLID application provided by an application provider. The application retrieves the user's pod from the identity profile. It then follows links from the profile to retrieve data on the user's pod and other pods, performing authentication as required.

choose to connect their pods to web applications by giving access to their data pods. The users themselves control the ownership and authority.

Thus, SOLID functions as a straightforward yet effective data management tool for individuals. Applications built using SOLID can read data directly from these data pods. By giving access control to users, SOLID promotes data security and simplifies the development of personal data governance.

To summarise, this chapter examines the theoretical foundations of the research, including information black hole theory, concepts of decentralisation, and principles of the semantic web. These concepts serve as a root for further study, providing an overall understanding of the related subjects.

# 3 Research Methodology

This chapter outlines the approach to address the research questions and sub-questions of this thesis. The study employs a combination of qualitative research techniques, including in-depth interviews and collaborative co-creation workshops, to gain a thorough understanding of user needs and preferences. Furthermore, we incorporate engineering principles and prototyping methods to create innovative solutions specifically designed to meet the identified needs. Table 1 1 presents the methods used to gather the essential data required for answering each research question.

| Research Question | Method |
|---|---|
| What is the current information exchange situation for refugees, and what are their needs? | Qualitative Study |
| What are the key features and functionalities required to improve the accessibility of this SOLID application? | Qualitative Study |
| How can a safe system be designed to broadcast information among refugees effectively | Design Study |
| What are the system's functionalities, and how do they align with its intended purpose? | Design Study, Qualitative Study |

Table 1: Research questions and corresponding methods.

## 3.1 Research Design Map

The design research map is described by two dimensions: One is defined by approach, and the other is defined by mindset [28]. Approaches to design research have come from a research-led perspective and a design-led perspective. Two opposing mindsets are evident in the practice of design research today: the expert mindset and the participatory mindset. Design researchers who have a participatory mindset value people as co-creators in the design process. In a participatory mindset, people are true experts in domains of experience such as living, learning, working [28]. In our research design, we utilised this design map to help us detail the research structure. It combined the expert and participatory mindsets, involving users in the system design, so that the system could be better tailored to users' needs.

## 3.2 Gathering Data from Interviews

Interviews were conducted in the formats selected by the participants, mostly using online platforms. This choice allows participants to take interviews in a convenient and comfortable setting. Anonymity was carefully considered throughout the process; each interviewee was informed about the confidentiality measures and confirmed their understanding and agreement to these terms before the interview began. This approach

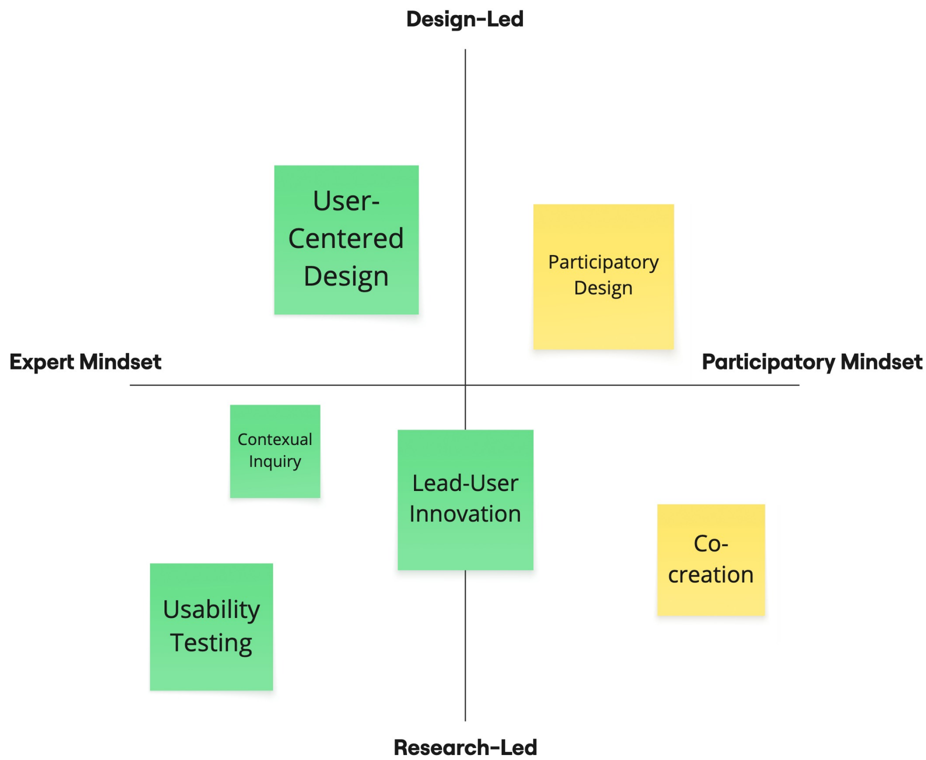



Figure 4: Research Design Map [28].

fostered a sense of safety and encouraged honest responses.

Interviewees came from mixed backgrounds, including refugees, workers from NGO, and academic researchers specialising in the relevant fields. As there exists a lot of mistrust among the refugee group, it's not easy to have direct conversations with them. We chose to contact intermediaries that they trusted to get in touch with them. For example, we had conversations with social workers who work closely with refugees. They also pointed out that due to privacy concerns, they always needed to understand the interviewers' background and their purpose entirely. Afterwards, the interviewers could be introduced to refugees for further interviews. We participated in humanitarian meetings and introduced our academic purpose to create a trusted environment where we could meet with them.

Semi-structured interviews were conducted to gather comprehensive insights, using open-ended questions designed to promote engagement. This format enabled participants to express their viewpoints based on their own experience, encouraging an environment where people can share their personal views freely. These interviews offer a unique chance to gain practical insights from individuals with first-hand experience, enhancing the data collection process.

## 3.3 Current Information Exchange Situation of Refugees and Their Needs

In this section, we thoroughly explored the specific requirements and needs of Eritrean refugees currently residing in Libya. To achieve this, we employed qualitative research methods, including a series of in-depth interviews and a co-creation session with participants from diverse backgrounds. Interviews and the co-creation were conducted in English and transcribed. To analyse the gathered data, thematic coding was used to translate the key points from the sentences. These focused on understanding the specific barriers that refugees encounter when seeking assistance, including challenges such as the lack of access to reliable information and contact issues within aid organisations. Interviewees also expressed the various help they require, ranging from legal assistance to mental health support. Additionally, participants shared their perspectives on privacy concerns related to sharing personal information online, expressing concerns about data security, potential misuse of their information, and the importance of their safety and anonymity.

Overall, this research aimed to provide a solution to the current issues faced by refugees. By focusing on these essential aspects, we aim to contribute to the development of support systems that address the complex situations faced by Eritrean refugees in Libya.

## 3.4 Key Features and Functionalities Required for the Application

To thoroughly capture the essential information, it's crucial for this study to assess the features needed by the user group. During this research phase, we analysed the results from the co-creation session that was conducted with a diverse group of NGO workers and data management experts, bringing together their unique perspectives and expertise. The session featured a series of open-ended questions designed to delve deeply into the specific needs and challenges faced by refugees.

In addition to exploring their experiences, the discussion emphasised the importance of employing data security measures to protect sensitive information about refugee identities. Participants shared insights on potential exposures and the ethical implications of data handling. As a result of this collaborative effort, key requirements for the proposed data management system were identified, including user-friendly interfaces, encryption protocols, and compliance with international data protection standards. These measures are aimed at enhancing both providing assistance and safeguarding data privacy.

## 3.5 Design a Safe System to Help Refugees Broadcast Information Effectively

The system building followed a design study methodology containing multiple stages. Initially, specifications and requirements were collected by analysing the interview data and the co-creation insights summarised in the earlier section. This analysis emphasised current data sharing practices, existing obstacles, and possible solutions. The participants' needs and expectations were considered to define a clear framework. Following these specifications, the system development phase began with an investigation of existing SOLID tools and methodologies.

The system was designed and developed utilising SOLID principles and RDF technologies to ensure a robust and scalable architecture. Python was employed as the primary programming language for building the dashboard, enabling interactive visualisations and efficient data processing. This combination of technologies enabled the decentralised data storage and enhanced the user experience through an intuitive interface.

## 3.6 Test and Evaluation of the System

Once the system has been developed, a comprehensive evaluation was conducted based on the proposed structure. This process includes a thorough technical evaluation of the framework, utilising a sample dataset that reflects the real situations of refugees. The system performance was then assessed with various user groups, including organisation representatives. These sessions aimed to gather practical feedback to measure user satisfaction and system usability. The feedback collected during testing sessions was documented, highlighting strengths and identifying areas for future improvement. This evaluation session is crucial for understanding the system's functionalities in real contexts.

Furthermore, the proposed system aims to present to participants the actual benefits of implementing SOLID technologies, emphasising how this framework facilitates data exchange. By improving communication and collaboration between refugees and organisations, the framework aims to provide a clearer understanding of how technology can bridge gaps and foster communication between humanitarian organisations.

In conclusion, this chapter discusses the research methods employed in the research process, including a research design map and how each research question was addressed. Qualitative approaches, design study, and engineering methods were utilised to explore the problems thoroughly.

# 4 Current Information Exchange Situation of Refugees and Their Needs

The main goal of this chapter is to thoroughly understand the current information-sharing situation of refugees and what their needs are. To address this research question, we talked with five individuals involved in refugee protection, including a refugee, a worker for a NGO, and academic researchers. Interviews 1 to 4 were done together with my Field Lab members from the Data Science in Practice course. Additionally, a collaborative session was organised with a group of individuals working in the field of refugee protection to discuss the application's needs. This chapter is organised to thoroughly examine and present the findings obtained from these interviews, aiming to align with and answer the research questions.

## 4.1 Present State of Data Exchange for Refugees

The current data-sharing format for refugees is mainly problematic, particularly in the context of Eritrea. In a recent interview, a key informant highlighted significant challenges related to data management and technology in the region. The interviewee pointed out that there is a lack of modern technological tools and proper database systems in place. As a result, the process of recording and sharing personal information about refugees is inefficient. The absence of digital records makes it difficult to exchange information securely, impeding the ability of organisations and agencies to respond effectively to the needs of refugees.

> *(Interviewee 3, refugee, video call, with JW and field lab members, 9 October 2024) I have no medical certificate and no passport. In my home town, there's no database. When I came to the Netherlands on a political trip, the only medical check I had was for tuberculosis. My information was on paper, and I shared it with the Dutch government.*

The interviewee we spoke with expressed concerns regarding the way organisations manage and protect their data. Specifically, they highlighted instances of data breaches and the lack of transparency about how personal information is stored and utilised. As a result, they indicated a preference for selectively sharing only certain information, rather than providing full access to their data. This approach allows them to maintain a degree of privacy while still engaging with the organisations in the early stage.

> *(Interviewee 3, refugee, video call, with JW and field lab members, 9 October 2024) I don't completely trust databases. They can be hacked, and there's a chance the data could be stolen. They're not 100% secure. I'm willing to share my passport and medical information with responsible organisations, but only partially. I want to keep some information to myself.*

When asked about their feelings regarding the use of an app that requires a password to manage personal data, the interviewee conveyed a positive attitude toward such platforms. They emphasised that using a secure application would not only enhance communication but also provide a sense of safety and control over their personal data. Additionally, they expressed a strong preference for using the application in their mother tongue, as this would enhance user experience.

> *(Interviewee 3, refugee, video call, with JW and field lab members, 9 October 2024) It would be good. When I'm at the doctor, they can find my registration by entering my name and birthday. If the app could be in my language, it would make communication easier.*

In summary, a notable gap exists in the current information-sharing platforms used by refugees, highlighting a critical need for improvement. The absence of digital databases and related technologies contributes to the ”information black hole”, where resources and support are inaccessible. While interviewees express uncertainty regarding the safety and privacy of their personal information when using digital tools, they are still willing to engage with these platforms. They see the potential for such technologies to help manage their personal data and communicate with organisations. This highlights the need for utilising digital tools to protect sensitive information.

## 4.2 Existing Barriers

One interviewee highlighted a potential challenge that could arise if the application is introduced to refugees. A focus must be on fostering trust within the communities and among the social organisations. This involves addressing the concerns that refugees may have regarding new technologies. It's essential to educate them about the importance of digital platforms in enhancing their access to resources. Additionally, we should clearly communicate the measures taken to protect their data privacy, such as encryption protocols and user consent practices. By prioritising transparency and building rapport, we can promote the use of the application.

> *(Interviewee 1, SOLID project builder, voice call, with JW and field lab members, 23 September 2024) It's trust. There is a gap in how refugees can trust that this application can guarantee their data security. Education is just one factor; it's also important to help refugees understand the application and ensure they can use it effectively.*

During our interview, we encountered a noteworthy situation when we asked the interviewee about data security. It became apparent that their understanding of the term ”data” was rather ambiguous, driving us to shift our focus to inquiries about physical documents instead. The interviewee highlighted that this is not an uncommon scenario; many refugees are often hesitant to engage with the concept of data due to their previous experiences, leading to a notable lack of trust. They conveyed that refugees frequently fear for the security of their personal information and are particularly anxious about losing vital documents, such as identification papers. This insight emphasises the challenges that arise in data security, particularly within vulnerable populations.

> *(Interviewee 4, researcher, video call, with JW and field lab members, 10 October 2024) That's common. When people start with some confusion, they tend to continue down that path. It's not always about what they have but what they think is important. Many refugees don't carry documents because they fear they will be lost or stolen.*

The gap between individuals' knowledge and their ability to apply that knowledge effectively often leads to distrust and misunderstanding. The interviewee highlighted that many refugees have very limited access to essential technology, which hinders their ability to access necessary resources. By implementing tailored solutions that consider these limitations, we can foster a more inclusive environment that helps bridge the gap.

*(Interviewee 4, researcher, video call, with JW and field lab members, 10 October 2024) This often happens when there's a gap between the people designing the system and the users. Refugees come from countries with limited access to technology, so the services we create need to be tailored to their unique experiences and needs.*

Barriers exist between the support systems and refugees who lack access to digital technologies, creating obstacles to assistance. These barriers often stem from inadequate resources that are designed for refugees. Fulfilling trust among refugees and developing systems that align with their needs is essential to bridge this gap. By prioritising an understanding of their situations, we can create more effective ways to enhance refugees' access to aid resources.

### 4.3 The Need for Receiving Information

Receiving efficient and accurate information is crucial in terms of humanitarian assistance. An interviewee who works for an NGO emphasises the importance of understanding refugees' specific needs and circumstances. NGOs can effectively tailor their programs by gathering relevant data, such as their health status, living conditions, and access to essential resources. This targeted approach ensures that appropriate solutions are implemented, enabling organisations to respond more efficiently to emerging challenges. This allows humanitarian efforts to be proactive in addressing the issues that refugees face.

*(Interviewee 5, NGO worker, video call, with JW, 24 April 2025) We need to know about the background information, because there's no way you can support someone without understanding where they are coming from, why they are passing through this and how they can overcome this challenge. So, information is quite great when determining how to design our program. We always need to design a program depending on the community that needs this information.*

The interviewee also noted that documentation is related to several issues, including employment and personal development. It is crucial for refugees to have access to professional training, education, and the job market. Moreover, they should be able to pursue job opportunities without any limitations despite their refugee background.

*(Interviewee 5, NGO worker, video call, with JW, 24 April 2025) Basically, it goes with the issue of documentation under protection. The documentation issue comes across other issues, such as job and improvement. Most of the things they are looking at are things that can help them economically. So access to proper and professional training, access to quality education, and, of course, access to market spaces where they can be able to compete in terms of selling their products, but again, be able to access jobs that are available without any restriction due to the status of the document that they hold.*

Refugees encounter significant communication barriers that hinder their ability to contact assistance organisations. Additionally, the lack of access to appropriate technology, such as smartphones and the internet, exacerbates these challenges. These factors prevent them from obtaining crucial information, accessing resources and support. Figure 5 offers a comprehensive overview of the identified obstacles. Without these technologies, refugees struggle to get information about legal assistance, health services, housing options, and educational opportunities. This combination of communication barriers and technological challenges hinders their ability to access timely help.

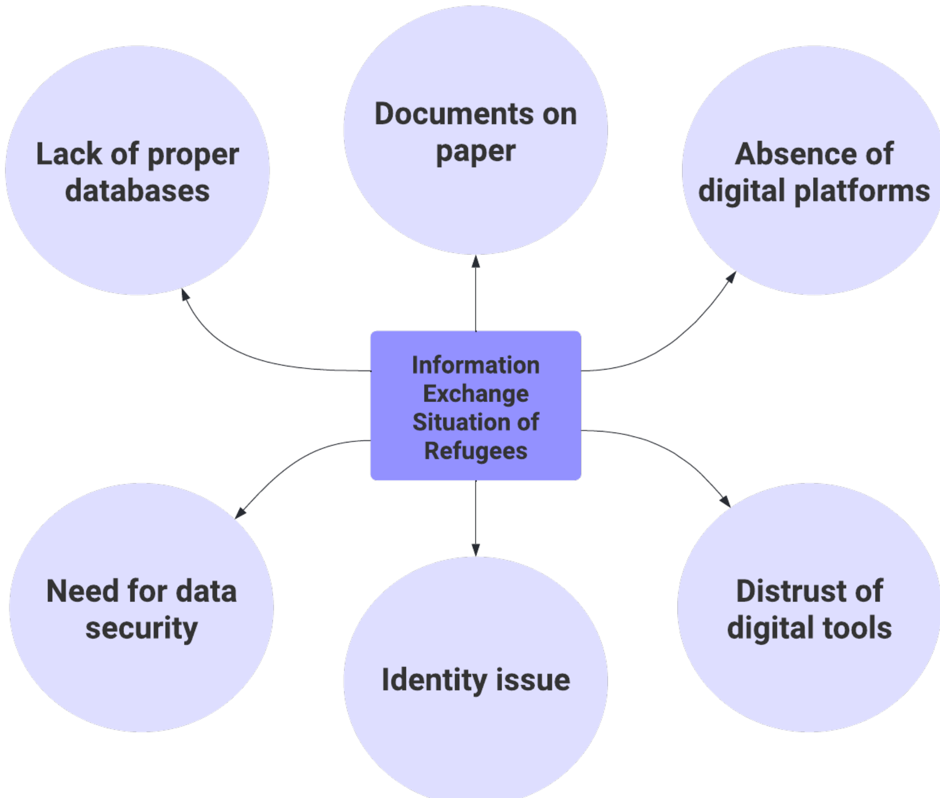



Figure 5: An overview of the current information sharing situation of refugees.

After assessing the current information exchange situation for refugees and recognising the urgent need for effective communication, it's crucial to identify the necessary functionalities of the system. The system will be designed to meet the actual needs of refugees, ensuring that essential information is accessible.

To tailor the application to users' specific needs, we organised a co-creation session dedicated to exploring the desired functionalities. This online session was held on 4 April 2025, which brought together a diverse group of professionals engaged in refugee protection, including social workers, legal aid specialists, and representatives from NGOs.

We started the session with an introduction to the SOLID principles, emphasising their significance in ensuring data protection and enhancing interoperability. We outlined the benefits of implementing these principles, illustrating their relevance through real-world use cases. Following this foundational discussion, we presented our primary application structure, along with a live demonstration of the current technical prototype, which allowed participants to understand the proposed functionalities.

During the session, all attendees were encouraged to share their insights and feedback. In the previous interview session, one interviewee highlighted that SOLID's interoperability feature facilitates secure and efficient data exchange among various systems, which is important for providing support to refugees.

> *(Interviewee 2, SOLID project builder, voice call, with JW and field lab members, 23 September 2024) The interaction between the public layer and external platforms. The interoperability issue concerns ensuring that the external systems' data in this layer is readable and formatted correctly.*

Building on this insightful comment, we engaged in a brainstorming session to identify potential technical solutions that could bridge the communication gap between refugees and public services.

### 4.4 Urgent and Common Needs to Highlight

Initially, we had a discussion focused on identifying the needs within the refugee group. During this meeting, we explored various aspects such as location, travel history, the year of arrival in the host country, and future plans. Those involved in this workgroup actively contributed their thoughts and experiences. One participant highlighted that, beyond gathering personal data, there is a demand for financial assistance and psychosocial support. This call for enhanced support underlines the importance of a holistic approach to address the well-being of refugees.

> *Beyond paperwork and documentation, asylum seekers and refugees need additional support, including psychosocial support and economic inclusion in terms of access to financial services, such as loans. Integration with national services is important.*

Another participant emphasised the importance of gaining acceptance in labour markets. It is crucial for refugees to be able to live independently.

> *I think what could also help is access to marketable skills, and also considering the restriction of movement, like it may take some time to get travel documents. They should have access to digital skills, so they're able to work.*

Figure 6 provides a comprehensive overview of the information that is necessary for providing humanitarian assistance. This includes personal details such as names, ages, and nationalities, as well as various social needs. It can significantly impact the effectiveness of assistance programs. By incorporating these diverse needs, humanitarian agencies can foster a more inclusive approach to support refugees.

### 4.5 Choose Who Can View Requests

Next, we will examine whether requests from refugees should be made accessible to the general public or restricted only to NGO workers. In the current draft system design, the querying function and knowledge graphs are configured to be open to anyone who has access to the dashboard. However, during the co-creation

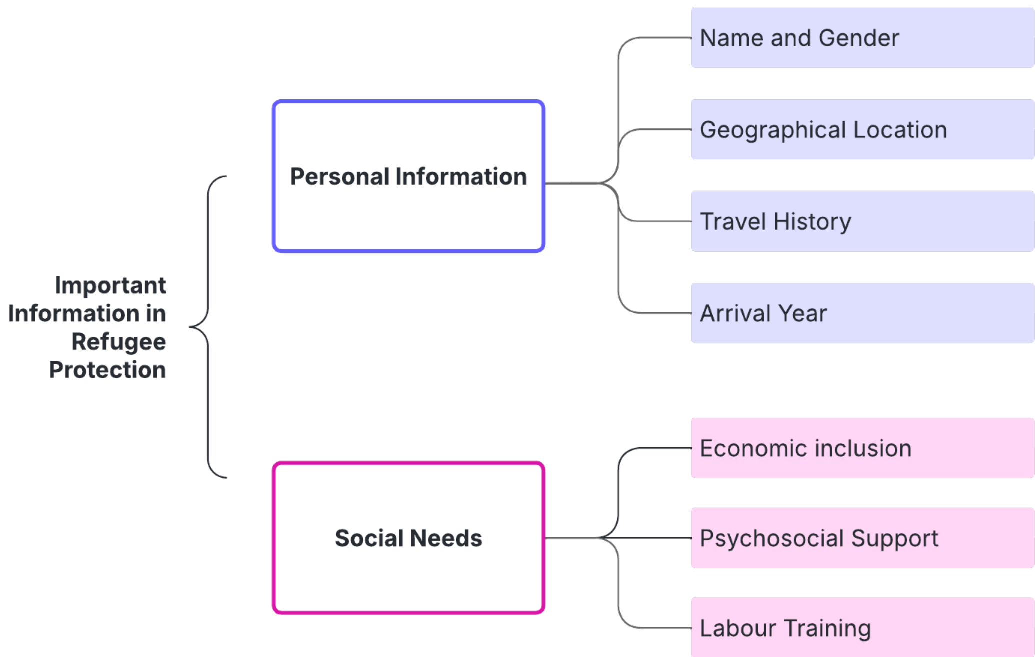



Figure 6: Identified needs in refugee protection from co-creation discussion.

session, one attendee raised a critical point: NGOs, given their role and expertise in providing aid, should have access to more detailed information than what is available to the general public.

> *I think the goal is to allow fellow stakeholders to access the information. It should be different for each person. Aid workers and other NGO's may need more information than the general public. The system should be set up so that it segments who gets what. There should be an option to either reveal the identity or remain anonymous.*

This differentiated access is crucial for enhancing the effectiveness of their interventions while ensuring that sensitive information is kept confidential. By implementing this approach, we can protect the privacy of refugees while providing them with the necessary assistance.

## 4.6 Set Appropriate Data Access

After identifying the required information and defining the target users, we proceeded to address the issue of ensuring data privacy through the identification method. One group member emphasised the importance of implementing an identification process before granting access to sensitive data. They argued that this pre-access identification is essential for safeguarding individuals' privacy and plays a key role in effectively using the data.

> *It's usually important that there's a level of identification, not necessarily everything, but an anonymity level that would make the data useful, depending on what objective the person has.*

By ensuring that only authorised users can access such information, we can take informed and responsible actions. This discussion highlighted the balance between accessibility and security. It helped define a clear framework that addresses both the ethical considerations and practical requirements of handling sensitive data.

A fellow attendee emphasised the critical need to safeguard the biographical data of refugees, highlighting that this information must always be kept confidential and anonymous. Such biographical data may include sensitive details, such as the refugee's full name, residential address, date of birth, educational qualifications, and work history. Protecting this information is vital to ensure the safety and dignity of refugees, as exposure could lead to potential threats. Implementing data protection measures and protocols is essential for refugee protection.

> *We always need to be careful about not sharing the biographical data of refugees. It shouldn't always be exposed to anyone. So what we do is we always anonymise our data, give them calls and other identification methods as well, and remove any biometric data. If we have an identity background, we will always anonymise that information. And it's very critical to the protection of the refugees.*

In our previous discussions regarding access to sensitive data, one of the co-creators emphasised the need to establish clear identity verification procedures for individuals with access to this information. Implementing robust credentialing measures, such as multi-factor authentication, during the login process can significantly enhance security. Additionally, to mitigate the risk of data leakage and enhance overall security protocols, conducting regular audits and systematically updating credentials is essential. By adopting these comprehensive strategies, we can ensure the privacy of refugees' sensitive data.

> *We need to ensure that this is a government person and not someone who was playing the other government person to access that amount of information. Even at the very beginning, when you're giving these credentials and letting them know that confidentiality is one of the main things that you're looking at, the person in the organisation is the only one who wants access to that information. And then you usually have things like changing the credentials occasionally. A regular check is also needed to ensure that the person who requested access from the beginning still has access to this information. Use periodic checks to ensure the data is given in the entrusted sequence.*

We proposed implementing several measures to safeguard refugee information and guarantee that it is accessed only by authorised people. Firstly, we should set an identification process that verifies the identity of users before granting access to the data. This will help ensure that only legitimate personnel can view sensitive information. Additionally, it is essential to maintain anonymity concerning biographical details, protecting the privacy of refugees. Lastly, implementing regular updates to credentials will further enhance security, making it more challenging for unauthorised users to exploit the data. Together, these features will create a secure framework for managing refugee data. Figure 7 illustrates various effective strategies designed to enhance data safety and protect sensitive information.

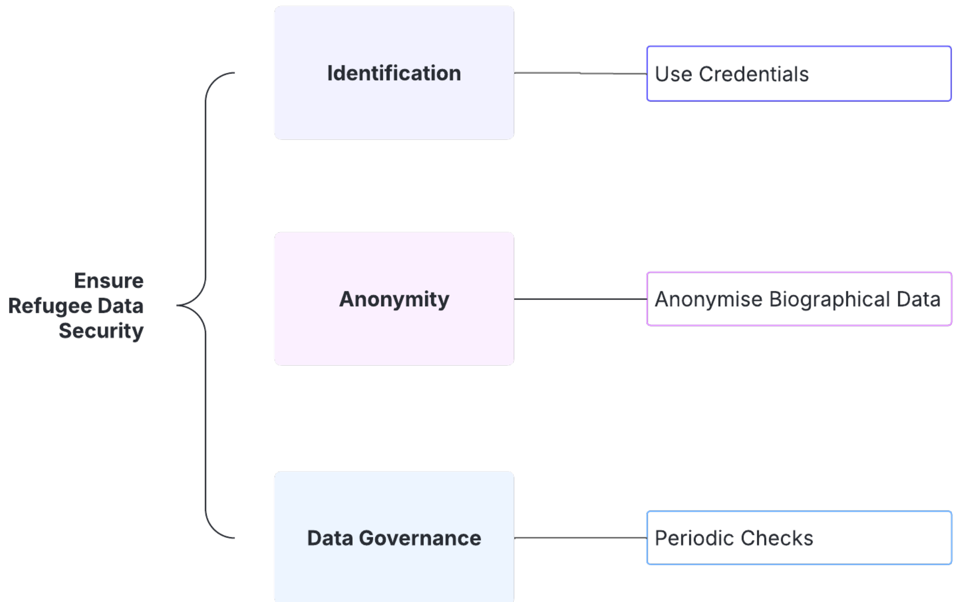



Figure 7: Proposed methods by co-creation group members to protect data safety. These solutions include implementing authentication protocols, conducting regular security audits, and enabling anonymity for biographical data for data protection.

In summary, based on the co-creation discussion, we have identified the key points that should be highlighted for the system design:

- Emphasise the most urgent needs of refugees. By addressing these identified issues, the communication gap can be narrowed.
- Ensure data is managed correctly, that is, only visible to the governance person with credentials. Organisations can thus reduce the risk of potential breaches and unauthorised access.

To improve our system, it is crucial to incorporate suggestions from people in the field of refugee protection. This approach enables us to ensure that our solutions effectively address real-world issues.

In this chapter, we delve into the specific information requirements and needs of Eritrean refugees to gain a comprehensive understanding of their unique circumstances. By assessing the barriers they face in obtaining essential resources and support systems, we aim to identify and highlight critical gaps in information sharing. Through interviews and the co-creation session, we gathered qualitative data to better understand the urgency of addressing their informational needs.

# 5 Key Features and Functionalities Required for the Application

The interviews and co-creation session with refugees, researchers, and NGO workers in the field of refugee protection provided valuable insights for the system design. This chapter will translate the data gathered during these sessions into actionable requirements, ensuring that the system addresses the actual needs of users.

## 5.1 Create Digital Databases

In previous interviews, participants emphasised the challenges faced by refugees due to a scarcity of digital platforms designed to support their specific needs. Many refugees rely on paper documentation, which leaves their personal information vulnerable to theft or loss. Their sensitive information could be duplicated during data exchange, posing a threat to information security. This reliance on physical documents also creates barriers to efficient communication. Thus, it can be concluded that building a digital database for refugees to store personal information is vital to bridging the information exchange gap. It enhances the efficiency of information exchange among humanitarian organisations and refugees. Such a system would help streamline assistance for refugees.

A digital database could ensure social workers have access to up-to-date records, facilitating support and co-operation. By integrating features such as data encryption and privacy controls, the database can safeguard sensitive information and ensure that refugees feel safe about sharing their details. Additionally, having a reliable digital system would allow faster responses to requests. It would also facilitate the process of following the route of refugees.

Overall, establishing such a digital database is a crucial step towards digitalisation for refugees. They can have control over their personal information, and receive humanitarian response in times of emergency.

## 5.2 Foster Trust Among Refugees

Interviewees pointed out that trust is a major obstacle in the field of refugee assistance. It is difficult for refugees to try possible technical solutions that are intended to help them because of the existing doubts about digital tools. This mistrust can be caused by the unfamiliarity with digital platforms and worries about data security. For example, refugees may be concerned that their personal information may be misused, which may restrict humanitarian agencies' capacity to provide effective help and support.

As a result, it is critical to foster trust among refugees. Initiatives targeted at building trust in refugee communities must be prioritised. This could include discussions about the intended use of technology and education sessions to familiarise them with these tools. In the development and implementation stage, it's also vital to engage the active participation of refugees. By cultivating a trusting environment, the overall protection and support for refugees can be improved.

## 5.3 Provide Support and Access to Resources

According to interviewees, the situation is made more difficult by a lack of access to resources for aid, such as financial support, vocational training, and economic inclusion. The call for timely support highlights the urgent need for a comprehensive aid strategy that addresses the current challenges. Apart from providing support such as food, shelter, and medical care, long-term solutions should also be integrated into action plans. Vocational training is beneficial in rebuilding the lives of refugees, enabling them to live independently and contribute to communities. Mental health services are also crucial to help refugees cope with the trauma of the journey.

Thus, a holistic aid strategy should be designed to enhance the overall well-being of the refugee community. To effectively address the mentioned needs of refugees, the system should be designed to convey their requests to assistance organisations. This involves creating a communication tool that allows refugees to share their requirements and ensures that these messages are safely received by aid providers. The system should include features that allow refugees to report their problems and challenges as they arise, so it can foster connections between refugees and society.

## 5.4 Ensure Data Privacy

It can be concluded that the sensitive information of refugees must be managed with care to safeguard their privacy and security. Interviewees emphasised the crucial need to authenticate the user's identity through a verification process before having access to personal data. This measure is vital to prevent unauthorised access and potential misuse of information. Additionally, it was pointed out that biographical details, such as names, nationalities, should be kept anonymous. This is a crucial action for improving privacy, as the leakage of such information could cause harm to refugees. Interviewees also commented that we should conduct regular audits of credentials for data access to maintain information security.

Protecting sensitive information is vital to keep the safety and dignity of refugees, as any disclosure could result in discrimination and dangers. Enforcing data protection strategies and protocols is necessary, such as user authentication during the login process. Furthermore, to reduce the possibility of data breaches and strengthen overall security measures, regular audits and updating credentials are needed. By implementing these strategies, we can effectively optimise the protection of data privacy and foster trust and safety within refugee communities.

Figure 8 summarises the key features and functionalities for the system design, which were collected from the interviews and the co-creation session with refugees, NGO workers and researchers in the refugee protection field. In these sessions, interviewees highlighted the urge to build digital databases, provide support, foster trust, and protect data privacy. To tailor the system to the actual needs of users, we need to comprehensively consider their requirements.

In summary, this chapter transforms the qualitative data collected from interviews and the co-creation with users into requirements for the system. In the following chapter, we will combine these required features with the technical structure and design solutions to the identified problem.

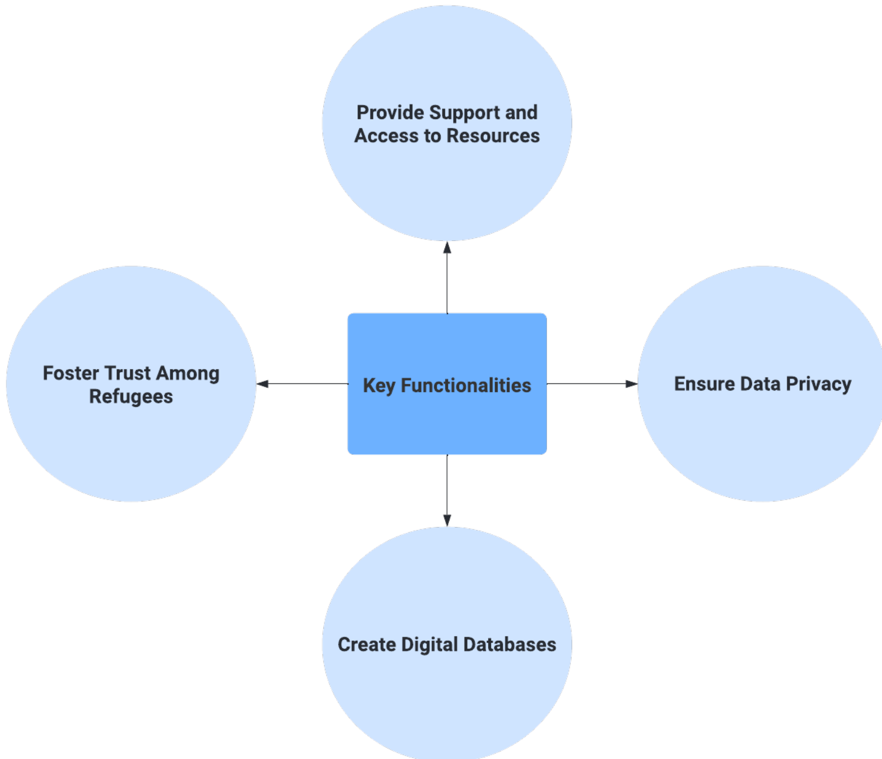



Figure 8: Key features and requirements gathered from users.

# 6 Design a Safe System to Help Refugees Broadcast Information Effectively

After thoroughly assessing the current barriers to effective information exchange for refugees, as well as the specific requirements for an efficient support system, we consolidated these insights into our system design. This chapter outlines the detailed architecture of the system, including its components and the implementation strategies employed. By addressing the identified challenges, we present a comprehensive solution aimed at facilitating seamless communication and access to essential resources for refugees.

## 6.1 Overview

We designed and built an information-broadcasting system aimed at bridging the communication gap between refugees and assistance organisations. This system is based on data gathered from interviews and a co-creation session and serves two user groups: refugees and NGO representatives. Refugee users log in through the SOLID App, which acts as a data-gathering tool with user authentication. The information and requests that refugees submit are stored in decentralised personal data pods and maintained in an RDF database. Once NGO users authenticate their identity, a Query Assistant will provide visualisations to help analyse the collected data. Figure 9 shows the overall structure of the data collection and analysis system. The following tools were utilised in this project: RDF, SOLID Pods, SPARQL, RDFLib, schema.org, and Inrupt development tools. This system demonstrates how SOLID data pods store refugee information in an

RDF structure, facilitating cross-platform and cross-application collaboration to achieve interoperability. It

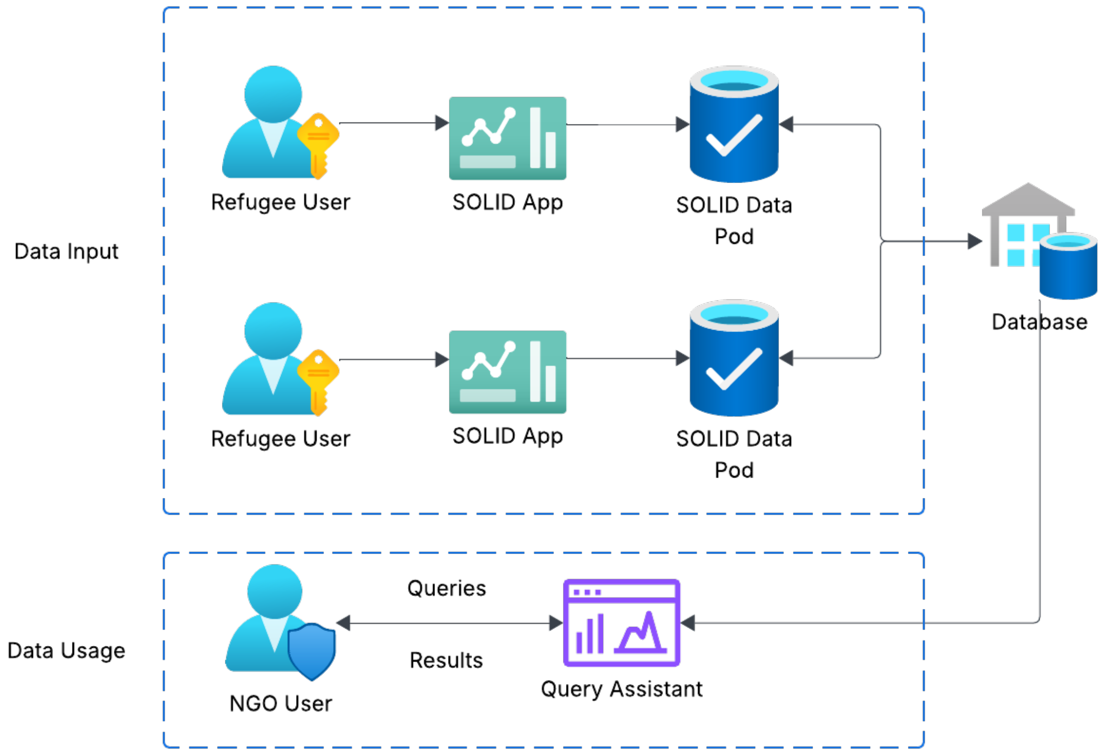



Figure 9: Overview of the system structure: Refugee users input data through the SOLID App, while NGO users can retrieve insights via the Query Assistant.

facilitates user authentication, data storage, and an interactive user interface:

1. *User Authentication.* Ensuring that users can securely access their SOLID pod through robust authentication methods. These measures enhance security by requiring users to provide multiple forms of identification before granting access.

2. *Data Storage Management.* Utilising the SOLID pod as a personal data store empowers users by granting them comprehensive control over their data. By leveraging the SOLID architecture, individuals can also ensure that their data remains secure, portable, and free from centralised data monopolies, fostering a more transparent and user-centric approach to personal data management.

3. *Application Layer Interface.* The design of the SOLID pod will feature a user-friendly interface that prioritises intuitive navigation and seamless interaction. This will include clear menus, easily accessible features, and a responsive layout tailored for various devices. By incorporating visual elements and simple prompts, users will be guided effortlessly through tasks, improving their overall experience.

These elements collaborate to establish a unified and safe setting in which users can efficiently handle their personal information, adhering to the privacy principles and user-focused design advocated by the SOLID protocol. Figure 10 shows the features and functionalities proposed by attendees of the interviews and the co-creation session. The system design fulfils the need to build a database, have connections to resources, and protect data security. However, due to limitations of the project scope and available resources, it is not feasible to provide technical education and build trust among the refugee group at the current development stage. The main achievements of the designed system are providing refugees with a safe platform to convey their needs and sharing the data insights with social assistance workers. Training sessions for technical platforms will be conducted in the future, thus making them familiar with such digital tools and fostering trust among refugees.


Figure 10: Checklist of requirements identified in the system design.

## 6.2 SOLID App Architecture

The primary focus of the SOLID App in this project revolves around the seamless interactions among the user, the application layer, and the user's personal SOLID pod. This interaction mechanism is firmly rooted in the SOLID protocol, which guarantees a clear delineation between the application layer and the underlying data storage. This separation is essential as it promotes enhanced privacy and security for users, ensuring that personal data is controlled and accessed only by the user themselves. The main components of this process include:

1. *User Login and Authorisation.* Under the SOLID protocol, users must authenticate themselves by signing in with their WebID to access the SOLID App, as shown in figure 11. When a user attempts to log in, the SOLID App sends a secure login request to the issuer of the user's WebID, typically the provider of the user's SOLID pod. The SOLID pod provider then processes this login request by verifying the user's credentials and assessing whether the user has the necessary permissions to proceed.

   Upon successful verification, the provider presents a detailed list of permissions requested by the

SOLID App, see figure 12. These permissions safeguard the user's data and ensure that the app only accesses information it genuinely needs. In the SOLID App developed for this project, the requested permissions include:

- Verify user's identity
- Run in the background
- View accessible user resources
- Act on the user's behalf

This structured permission request is crucial for maintaining user privacy and control over personal data while using the app. At this stage, the user faces an important decision: they can either accept or reject the authorisation request presented by the SOLID App. Should the user choose to deny the request, the entire authorisation process will be halted immediately, and as a result, the SOLID App will be unable to access or retrieve any data stored in the user's SOLID pod. This ensures that the user's privacy is maintained and no information is shared without explicit consent.

On the other hand, if the user opts to grant permission for the request, the SOLID pod will securely send back the user's identity information, including their unique identifier and the corresponding pod URI. The SOLID App will then utilise this information for various functionalities, such as personalising user experiences or securely exchanging data. The choice made by the user is critical, as it determines the extent of data sharing and interaction with their SOLID pod.

This process guarantees that users maintain complete control over their data. It empowers them to decide whether the SOLID App can access or write data to their personal pod. By putting data ownership in the hands of the users, it fosters trust and enhances privacy in digital interactions.

2. *User Data Submission and Data Storage.* Once the user grants the necessary permissions and chooses a specific pod for data storage, the process begins with the user accessing the SOLID App, which is designed for user-centric data management. In the app, the user will use an intuitive data-entry box to enter structured information. This includes essential details such as their name, geographic location, and postal code, among other pertinent data points that might be relevant to the context of the application.

   As the user inputs their information, it is dynamically organised into an RDF format. RDF is a standard model for data interchange on the web, specifically tailored to enhance data interoperability across different platforms and applications. Storing data in this format is critical as it allows for effective reuse and querying, making it easier for various systems to share and manipulate the information without compatibility issues.

Once the user has completed the data entry and clicked the submit button, the SOLID App processes this information efficiently. The application securely transfers and saves the entered details to the specified pod chosen by the user. Each piece of data recorded contains the user's input and is accompanied by a unique URI. This URI serves as a crucial compliance measure, ensuring that the data can be accessed and linked in a manner that maintains its integrity and adheres to established accessibility standards.

This structured and compliant approach not only empowers the user by giving them control over their personal data but also fosters an environment of trust, where the information can be easily retrieved and utilised across different applications while prioritising user privacy and data governance.

3. *Session Logout.* Once the RDF data has been successfully written and stored, if the user decides to shut down the SOLID app or remains inactive for an extended period, the system will automatically initiate a timeout protocol. During this timeout period, the application monitors user activity and, upon detecting inactivity, logs the user out to ensure security.

   When this occurs, the SOLID app reverts to its original state prior to the user's login. This restoration process not only safeguards the application's functionality but also protects against unauthorised access to the user's sensitive information. As a result, any potentially exposed data is well-protected, reinforcing the importance of maintaining user privacy and data integrity within the application.

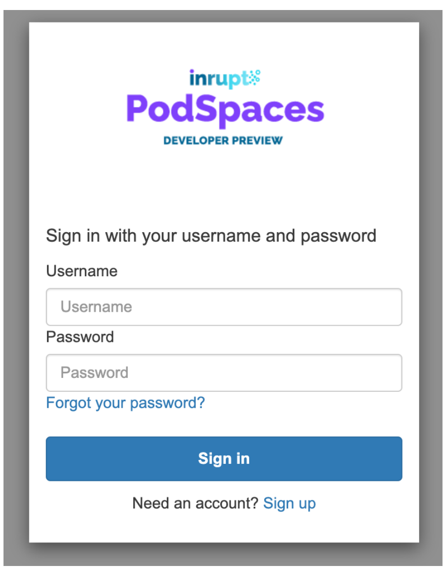



Figure 11: WebID Example when users log in. Source: https://podpro.dev/login

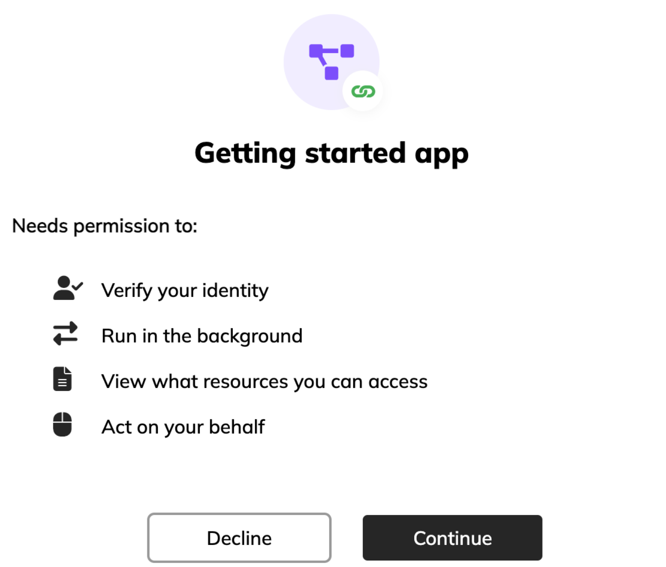



Figure 12: User permission example when accessing data. Source: https://login.inrupt.com/openid

By focusing on these critical components, the SOLID App aspires to cultivate a digital environment that significantly enhances user experience while simultaneously adhering to the standards of privacy and data security, in alignment with the principles of the SOLID protocol. This comprehensive approach encompasses a range of features designed to empower users, allowing them to navigate their digital lives with confidence and security. The SOLID App prioritises user autonomy by ensuring that individuals have complete control over their personal information. This control is foundational to the user experience, fostering a sense of trust and ownership. Moreover, the App implements advanced encryption techniques to safeguard personal data, ensuring that sensitive information remains private and protected from unauthorised access.

Overall, the SOLID App's holistic approach aims to deliver an exceptional user experience but also ensures that individuals can participate in the digital landscape, fully aware that their personal information is secure and under their control.

### 6.3 Implementation of the SOLID App

The SOLID App for this project was created using HTML, CSS, and JavaScript, primarily relying on Inrupt JavaScript libraries [1]. These APIs managed functions such as SOLID authentication and retrieving data from SOLID pods. PodSpaces [2] provides SOLID data pods for data storage. To get a WebID and a pod on PodSpaces, we followed these steps:

1. Visit PodSpaces.
2. To create an account, you need to accept Inrupt's Terms of Service. Please check the box to show your agreement.
3. If you accept Inrupt's Terms of Service, proceed by clicking the Sign Up button.
4. If you haven't registered with the Inrupt Identity Provider yet, click on the Sign up link to create a new account:
    - Enter your username, email, and password.
    - Click Sign up. A verification email will be sent to you.
    - Check your email for the verification message and follow the instructions to confirm your account.
    - After verifying, go back and select Continue to access the Sign in page, where you can enter your username and password. Then, click Sign in to access your account.

Figure 13 displays the login page of PodPro, where users can view data stored in SOLID data pods after entering their authentication details. We specify the WebID provider, which in this case is *https://login.inrupt.com/*, along with the username and credentials.

[1] https://docs.inrupt.com/developer-tools/javascript/client-libraries/tutorial/getting-started/
[2] https://docs.inrupt.com/pod-spaces/

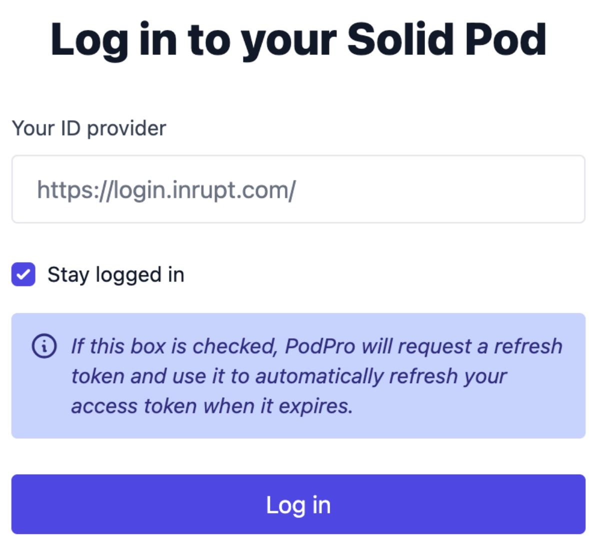



Figure 13: PodPro Login Page. Source: https://podpro.dev/login

The SOLID app uses npm [3] and webpack [4] to run locally on *http://localhost:8080/*. Once we got a pod, we could start the application-building process, which consisted of three stages: login, data input, and data storage.

1. *Login and Get Pod Address.* This part primarily uses Inrupt's `solid-client-authn-browser`[5] and `solid-client`[6] libraries. The execution depends on functions established in these libraries to manage sessions, facilitate login, redirect users, and obtain Pod locations according to the user's WebID. A WebID is a URL that identifies a user and dereferences to the user's WebID profile document. The login process is as follows:

    - Log in a user.
    - Reads the Pod URL(s) associated with the user's WebID.
    - Write a reading list for the user's Pod.

2. *RDF Data Input.* This section utilizes Inrupt's `solid-client` and `vocab-common-rdf`[7] libraries to generate RDF objects based on user input. Initially, the SOLID App verifies whether the relevant RDF data is already present in the Pod by employing functions designed to retrieve pod content as defined in `solid-client`. If RDF data is discovered, it is removed to permit the new information to take its place. When no existing data is found, functions aimed at creating datasets are invoked to establish an empty SOLID dataset in the specified pod location. Following that, when RDF data is produced from the user's questionnaire responses, the `vocab-common-rdf` library is utilised, which

[3] https://docs.npmjs.com/getting-started
[4] https://webpack.js.org/
[5] https://github.com/inrupt/solid-client-authn-js
[6] https://github.com/inrupt/solid-client-js
[7] https://github.com/inrupt/solid-common-vocab-rdf

includes several established vocabularies. For this project's SOLID App, Inrupt's adaptation of the schema.org [8] vocabulary is predominantly applied, featuring properties like `name`, `organisation`, `address`, `addressCountry`, and `postalCode`. The application of schema ensures that all identifiers are standardised and traceable, thus preventing issues of identifier inconsistency that could interfere with interoperability.

3. *Data Storage and Validation.* This part continues to use functions defined in Inrupt's `solid-client` API for saving RDF datasets to the specified location in the Pod and retrieving datasets. Upon successfully storing the data, a confirmation will be returned in the form of the dataset's name, signalling the completion of the operation.

Figure 14 shows the general workflow of the SOLID app. Users receive a WebID and link to their data pod on PodSpaces through email verification. They can write data using the SOLID app. The information is stored in PodPro; once the process is successful, the retrieved name will be displayed. To check the stored data on PodPro, users need a valid WebID and credentials.

Figure 15 illustrates the refugee log-in page of the SOLID app, designed specifically for users in need of a streamlined and secure way to access their personal data. Upon arriving at this page, refugee users are first prompted to select an identity provider from a list of SOLID data pod providers. This selection is crucial, as it establishes the link to their personal data stored in decentralised pods.

Once an identity provider is chosen, users must enter their unique WebIDs, which serve as identifiers that point to their corresponding data URLs within the pod. This process not only ensures a personalised and direct connection to their information but also reinforces the privacy and control users maintain over their data.

Figure 16 presents a user case example for the data write-in section. The SOLID data pod is selected using the pod URL given during the login process. Users are prompted to enter their information based on the provided example. After the data is stored in the personal data pods, the user's name will be retrieved to confirm the status of the process.

Figure 17 presents a detailed example of the RDF data format utilised within SOLID data pods. This schema format organises the input data into distinct categories: name, address, country, postal code, occupation, and specific needs. By structuring the data in this way, it not only allows for a comprehensive understanding among various users but also significantly enhances interoperability across different systems and platforms. Each category is designed to capture essential information that can be easily accessed and shared, thus fostering collaboration and ensuring that users can effectively communicate their requirements and preferences.

[8] https://schema.org/

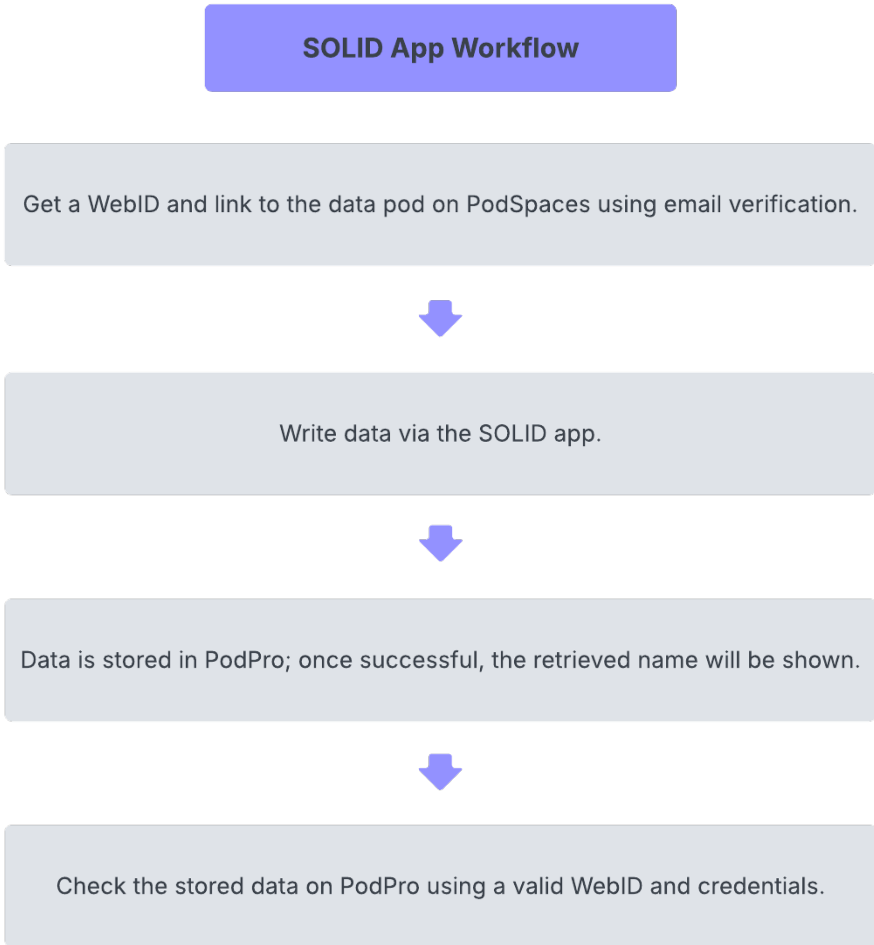



Figure 14: SOLID app workflow.

### 6.4 Query Assistant Architecture

Data contained in the RDF format within SOLID pods belonging to various refugees can be efficiently exported for analysis and application use. Although the fundamental RDF data is relatively straightforward to parse and is machine-readable, displaying good clarity in certain syntaxes such as Turtle format, it often requires additional processing to align better with human usage preferences, especially in dynamic applications.

One specific application scenario developed in this project involves the creation of a robust application that utilises RDF data in conjunction with identity authentication protocols. This application is designed to serve as an essential bridge between end-users and RDF datasets that contain crucial information regarding their situation. By implementing secure authentication measures, the application ensures that only authorised users, including stakeholders like organisations providing support to refugees, refugee coordinators, and case workers, can access sensitive data. Through this application, stakeholders can more effectively retrieve

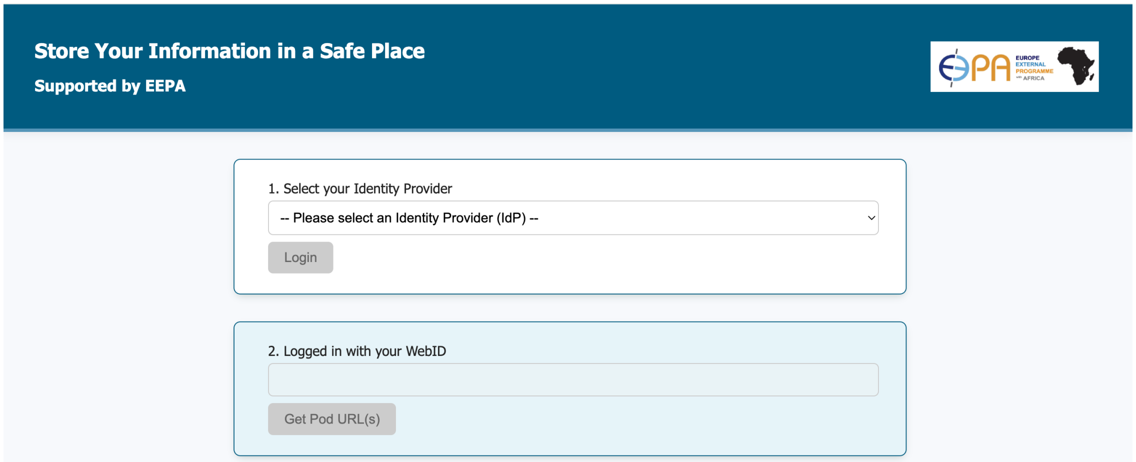



Figure 15: Refugees log in page.

vital information, such as the various forms of assistance required by refugees. It enables them to derive actionable insights from the raw data efficiently, fostering better-informed decision-making processes.

The information query function consists of three primary elements in the interface that enable users to interact with refugee data in a dynamic way, as shown in the figure 18: the user authentication, the querying feature and the knowledge graph feature.

1. *User Authentication.* Before gaining access to the personal data of refugees, users of the Query Assistant are required to follow a strict authentication process designed to protect sensitive information. Initially, users must select their organisation's name from a predefined list to ensure that the access request is being made by an authorised entity. Following this selection, they are prompted to enter a specific authentication code associated with their organisation.

   This authentication code serves as an additional layer of security, ensuring that only individuals with legitimate credentials can view the dashboard containing personal data. The system will verify the entered code against the organisation's records. In the event that users enter an incorrect code or fail to select an appropriate organisation, access to the dashboard will be denied. Figure 20 shows the login page of the Query Assistance. By restricting access to authorised personnel, the system works to prevent unauthorised usage and protect the rights of the refugees whose data is being handled.

2. *Execute Queries.* Users can obtain comprehensive information about a specific refugee by entering their name into the system. The platform incorporates a sophisticated query template selection feature, which empowers users to choose from a diverse array of query types tailored to their specific information needs. In this prototype demonstration, users have access to several querying options, including location, travel history, arrival year, and future plans, as shown in the figure 21. Each query type is linked to a pre-defined SPARQL query template that expertly generates SPARQL statements. These statements are crafted to dynamically retrieve corresponding RDF data from the underlying database, ensuring that users receive accurate and relevant information in real time.

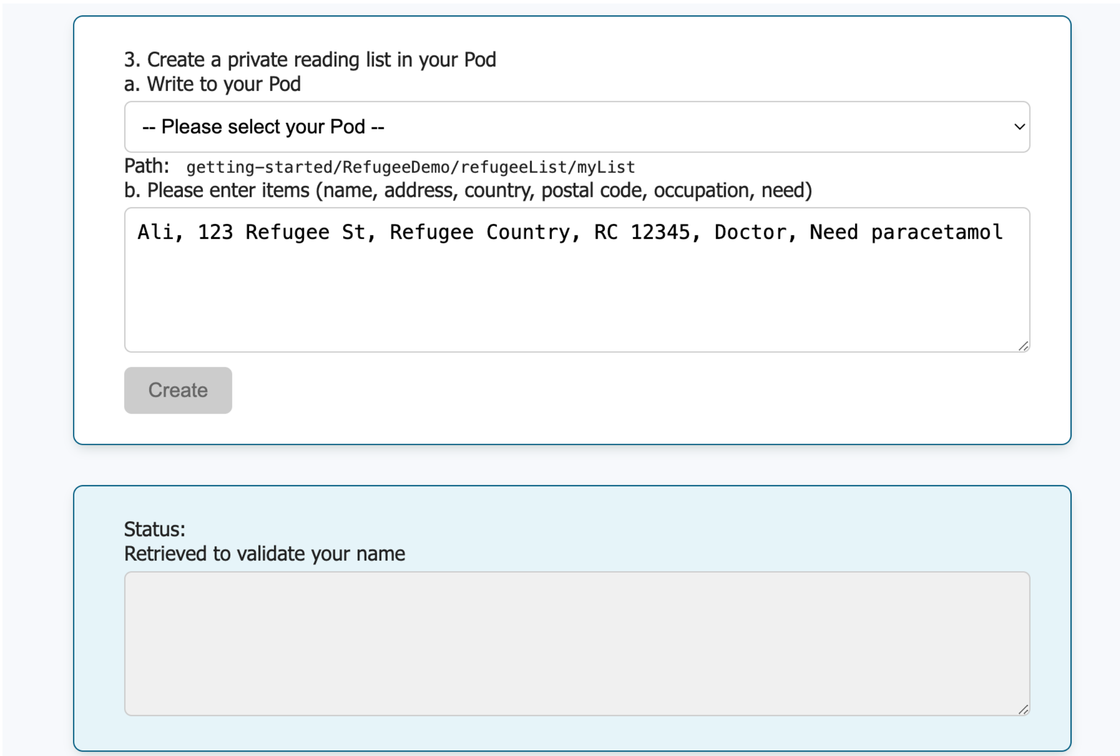



Figure 16: Write in refugee data.

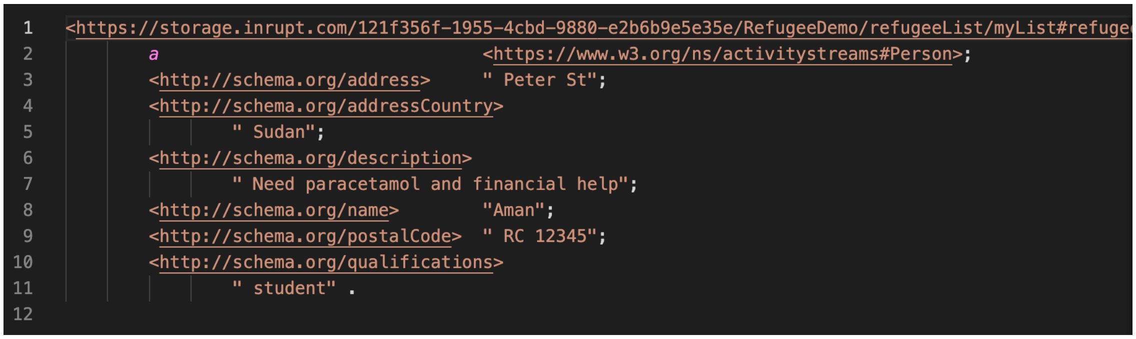
Once the user defines their query by selecting their preferred options and entering the name, they can click on the "Execute Query" button. This action initiates the retrieval process, generating specific results related to the entered name. The output is designed to be user-friendly, presenting the data in a clear and accessible manner.

3. *Generate Knowledge Graphs.* The Query Assistant constructs a comprehensive knowledge graph based on data sourced from the RDF format. This tool empowers users to visualise and explore the interconnected information as a knowledge graph. An example of the generated knowledge graph is shown in the figure 19. By doing so, it enhances their understanding of the relationships and associations between diverse data points, facilitating deeper insights and informed decision-making.

The Query Assistance assists various stakeholders, such as researchers, humanitarian workers, and policymakers, in understanding the complex issues surrounding refugees. By thoroughly examining the data, the platform helps users identify trends, challenges, and opportunities, ultimately aiding in informed decision-making and advocacy efforts.

## 6.5 Implementation of the Query Assistant

The Query Assistance is a sophisticated application developed in Python that encompasses three distinct yet interconnected modules: a graphical interface, RDF processing, and graph visualisation.



```
<https://storage.inrupt.com/121f356f-1955-4cbd-9880-e2b6b9e5e35e/RefugeeDemo/refugeeList/myList#refuge
        a                               <https://www.w3.org/ns/activitystreams#Person>;
        <http://schema.org/address>     " Peter St";
        <http://schema.org/addressCountry>
                " Sudan";
        <http://schema.org/description>
                " Need paracetamol and financial help";
        <http://schema.org/name>        "Aman";
        <http://schema.org/postalCode>  " RC 12345";
        <http://schema.org/qualifications>
                " student" .

```

Figure 17: RDF data example.

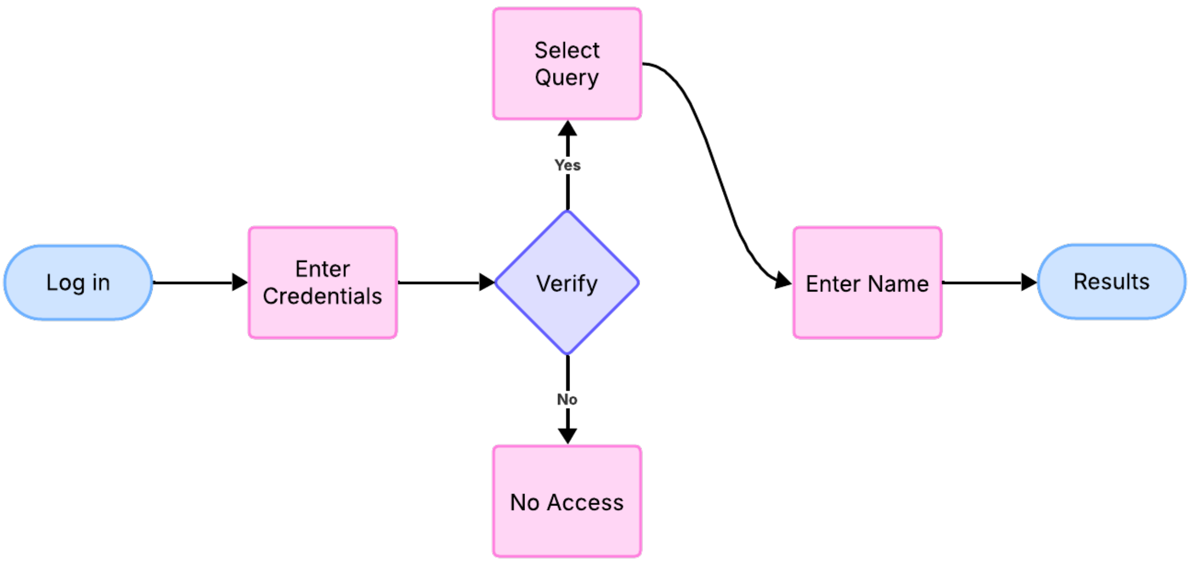



Figure 18: Workflow of Query Assistant.

1. *Graphical Interface.* The graphical interface is mainly created using the `Streamlit` [9] library, which allows for the rapid development of web applications specifically tailored for data science projects. Streamlit's interactive widgets, such as sliders, buttons, and text inputs, enhance user engagement by enabling users to easily manipulate inputs and view outputs in real-time. This interface is designed to provide users with an intuitive experience, making it easy to enter queries and visualise RDF data.

2. *RDF Processing.* The creation and query of RDF mock data uses the `RDFLib`[10] library, a powerful toolkit for working with RDF data in Python. Within this module, a key feature is the creation and querying of RDF mock data, which is structured in a way that simulates real-world refugee information.

[9]https://streamlit.io/
[10]https://rdflib.readthedocs.io/en/stable/


Figure 19: Knowledge graph example.

3. *Graph Visualisation.* For RDF visualisation, `NetworkX`[11] and `Matplotlib`[12] libraries are used. The `graph` module in `RDFLib` is mainly used to create an RDF `Graph` object containing refugee mock information. The query method is defined inside the `Graph` class, which allows queries using SPARQL, so different queries can be performed using predefined SPARQL templates for different needs. This class can also output raw RDF data in different formats through the `serialize()` method. In addition, the `NetworkX` library can be used to construct the corresponding nodes and edges in the directed graph by enumerating the subject, predicate, and object triples in the graph object. Each entity in the RDF graph corresponds to a node, and the relationships (predicates) are represented as edges connecting these nodes. The visualisation is further enhanced by combining methods from `Matplotlib`, which provides extensive capabilities for customising visual representations. This includes adjusting node sizes, colours, and layouts to improve clarity and detail, ultimately helping users to gain insights from the RDF data at a glance.

These combined modules form a cohesive and powerful application designed specifically to enhance user interaction with RDF data. They enable users to efficiently query, manipulate, and visualise this type of data in a manner that is both user-friendly and intuitive. By integrating different functionalities, the application streamlines processes and provides valuable tools for users. With its emphasis on usability, the application transforms complex RDF data into meaningful insights, fostering deeper understanding and facilitating informed decision-making based on structured information.

[11] https://networkx.org/
[12] https://matplotlib.org/

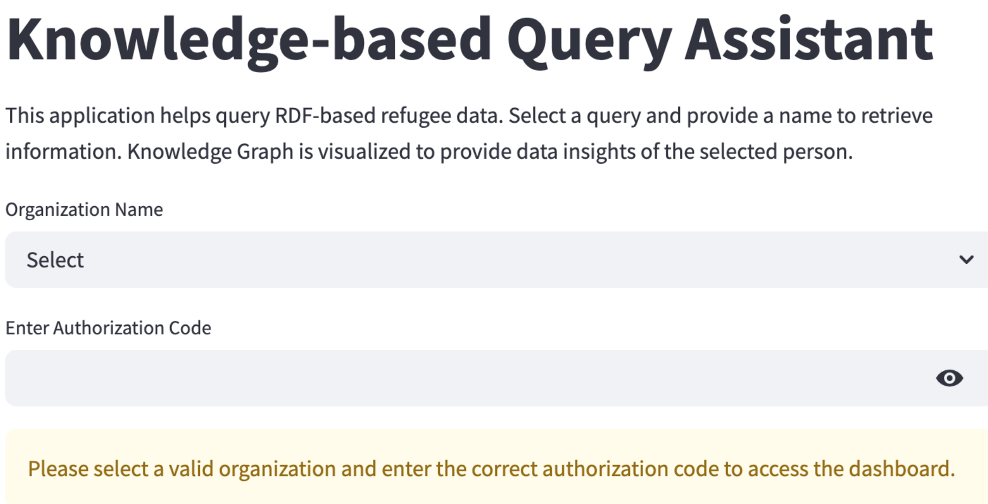



Figure 20: NGO user log in page of Query Assistant.

The SOLID app and the Query Assistant work together to form a robust ecosystem for data collection and analysis, tailored specifically to the needs of refugees. This integrated system not only facilitates the efficient sharing of vital information but also prioritises the privacy and security of users' personal data by leveraging advanced privacy protocols. The use of the RDF data format allows for a flexible and structured way to represent information, while the decentralised nature of SOLID data pods empowers users by giving them control over their own data. This architecture significantly enhances interoperability across various applications and platforms, ensuring that information can be seamlessly exchanged and utilised in a manner that supports the diverse needs of refugee populations. Overall, this innovative combination of technologies aims to create an effective information-broadcasting platform that is both user-centric and secure.

In conclusion, we provide a solution to address the information-sharing challenges faced by refugees. This chapter focuses on the system architecture and implementation details of the SOLID app and the Query Assistant. Example workflow and user pages were provided to help better understand the system's functionalities.

# 7 Test and Evaluation of the System

To thoroughly assess and validate the system's functionality, we evaluated the SOLID app and the Query Assistant. This evaluation explored the possibility of expanding the Schema vocabulary, integrating with the Semantic Web, and implementing automated RDF data storage and data security measures. Additionally, we gathered feedback from a group of users to gain insights based on their experiences and identify potential areas for future improvement.

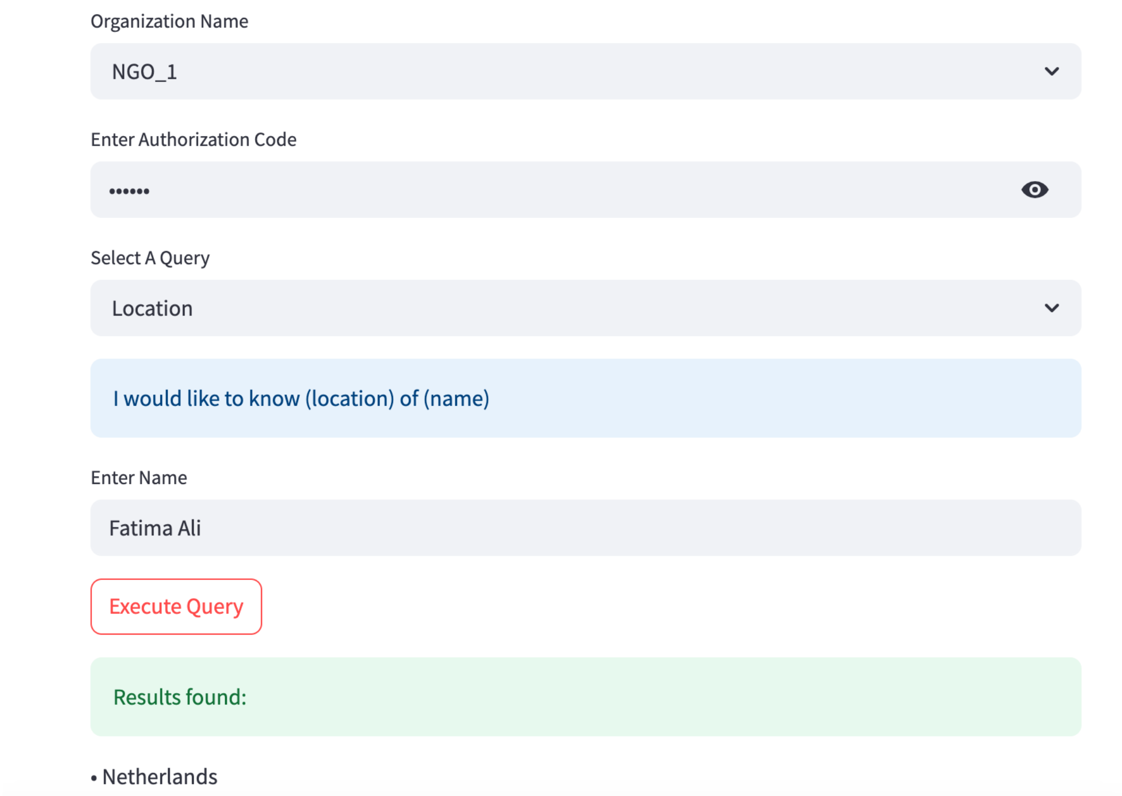



Figure 21: Querying page where users can retrieve information after selecting a query.

### 7.1 Schema Expansion and Standardisation

The adaptation of schema.org vocabularies for refugee needs is fundamental in ensuring accessible information exchange. This development has involved several key components:

- *Custom Fields Development.* Tailored existing schema.org terms to better reflect the requirements of refugees, such as specific housing, healthcare, and educational resources.
- *Global Interoperability.* Enhanced the interoperability of data collection, so that it can be shared and used across different platforms.
- *Data Consistency and Reliability.* Data integrity is crucial for organisations to ensure consistent and reliable information-sharing. It ultimately supports effective aid delivery. By implementing validation processes, we can safeguard the quality of the system and foster trust among stakeholders.
- *Standardised Data Entry.* Standardised methods and protocols for data collection were implemented to ensure consistent data collection across various platforms. Organisations can effectively gather and analyse information in a uniform format. This approach enhances the overall reliability of the data-driven processes.

## 7.2 Integration with Semantic Web Services

The primary goal of integration within the semantic web is to ensure compatibility and interoperability among various platforms. This feature is essential for creating a cohesive framework that effectively supports refugees. By enabling smooth communication and data exchange between different services, we can enhance the overall user experience.

- *Service Delivery Enhancement.* Different systems should be able to communicate and share information seamlessly. By improving the procedure of service delivery, we can reduce redundancies and foster collaboration across various sectors. This method also enhances the information sharing process.

- *Future Integration Opportunities.* This system has the potential to integrate with emerging technologies and provide a more efficient development process for future projects. Thereby, the overall productivity and innovation are enhanced.

This integrated approach streamlines access to information and fosters collaboration among organisations. It can also support the future development of similar systems used to address the diverse challenges faced by refugees.

## 7.3 Automation of RDF Generation and Storage

Automation plays a crucial role in managing data with both efficiency and security. This automated system for data entry and querying enhances accuracy by minimising human intervention. Additionally, automating data handling improves security measures, protecting sensitive information from potential breaches.

- *Automated Data Entry.* This system transforms user inputs directly into RDF format, ensuring the raw data can be converted into a structure that is understandable by machines. This process enhances data interoperability, allowing systems to share and use information effectively.

- *Security and Data Integrity.* Security protocols are integrated into system design to help safeguard sensitive data from unauthorised access. User authentication promotes data security, ensuring that the data management process meets compliance and privacy standards.

## 7.4 Data Security Measures

Sensitive information is protected through security procedures designed to maintain data confidentiality. First, the system follows the SOLID authentication protocol, which requires users to verify their identity before accessing any data pods. This ensures that only authorised people can see sensitive information. Additionally, Query Assistant implements identity verification methods so that only users with the correct credentials can enter the system. Together, these security mechanisms create a safe environment, ensuring that personal data remains protected from unauthorised access and potential breaches.

- *Data Privacy.* User privacy is safeguarded through data protection methods, which adhere strictly to SOLID's protocols. These protocols ensure that all personal information is handled carefully, minimising risks and maintaining confidentiality. The system ensures that only authorised users can view or manage data. With these measures, users can trust that their data remains secure.
- *Compliance with International Standards.* The system implements a comprehensive framework to ensure that all data handling practices are fully compliant with the GDPR and the Malabo Convention. This includes security measures to protect personal data and maintain individuals' privacy rights carefully.

To sum up, in order to thoroughly evaluate and validate the system's functionality, we carried out a comprehensive assessment of both the SOLID app and the Query Assistant. This assessment explored the potential for expanding Schema vocabulary, integrating with the semantic web, automating RDF data storage, and implementing data security protocols. Through these analyses, we aimed to confirm that the system adhered to usability and reliability standards.

## 7.5 User Adoption

User tests were conducted among researchers and NGO workers after the technical implementation was completed to ensure the system's efficiency and practicality. The first part was held on 18 June 2025, focusing on gathering feedback on the system performance. The necessity for a free-text search function in Query Assistance, similar to Google Search, was highlighted in the user test. This would enable users to search for NGOs that address specific issues, such as human trafficking, in particular regions. Attendees explained that, since the majority of users are accustomed to free text search systems, this functionality was deemed necessary. Instead of only selecting from a limited list of NGOs, it would be more helpful to search for a relevant organisation when users require help.

The second part of the evaluation process was held on 24, 28 and 27 June 2025, with researchers from backgrounds in refugee protection and human trafficking. The meeting focused on the creation and use of a web ID for data entry, specifically for collecting refugee information. The process of selecting an identity provider, logging in, and entering details such as name, address, and country was explained to users before they attempted this process. This test was done using both a laptop and a mobile phone. Users emphasised the need for hands-on experience to better understand the system. They discussed the integration of the system with other data entry systems that other data stewards prefer. Concerns were raised about the app's user-friendliness, especially for non-tech-savvy users. They also emphasised the importance of introducing the app to users and explaining what to expect and how to use it, as it may be a bit complicated for new users. Moreover, if the human-machine interface is more intuitive, users could have more control over the applications. For instance, existing applications for refugees are typically managed by the United Nations or other international agencies. It's necessary that refugees have ownership of such applications.

Based on the received feedback in the user testing part, it can be concluded that future developments should focus on the following aspects:

1. Provide an expanded list of available humanitarian assistance organisations in the Query Assistance dashboard.
2. Provide education sessions to users without technical backgrounds, so that they can follow the SOLID App more easily.

The user evaluation provided valuable insights and feedback to the system design. The current technical structure was evaluated based on practical experience and previous work in the refugee protection sector, allowing us to make further enhancements and improvements to the system. We will seriously consider this feedback and make corresponding improvements in the subsequent development to ensure that the system can fully meet users' needs and provide them with better services.

To conclude, this chapter evaluated the functionality of the designed system, including schema vocabulary expansion, integration with the semantic web, RDF database and data security protection. User tests were carried out in preparation for future development.

# 8 Discussion

In this section, we present the key findings of our study, which provide valuable insights into the management and sharing of information related to refugees, particularly focusing on Eritrean refugees in Libya.

## 8.1 The Problem

The primary problem we aimed to address is the information black hole that refugees face, which stems from inadequate communication between refugees and humanitarian organisations. This challenge is especially prominent among Eritrean refugees in Libya, as their limited ability to communicate hinders them from expressing their needs. Therefore, it is crucial to make their personal information accessible while protecting their privacy.

To address this challenge, our research aims to improve the accessibility of personal information for refugees and enable efficient communication between support services. This initiative aims to empower refugees to get the timely assistance they need. We strive to bridge the communication gap among refugees and protect data privacy by utilising SOLID technology.

## 8.2 Key Findings

To begin, we explore the specific information needs of Eritrean refugees to gain a thorough understanding of their current situations. By examining the obstacles they encounter in accessing support, we seek to identify the communication gap that exists. Our qualitative data, collected through interviews, helps illustrate their experiences and understand the urgency of solving this problem.

To customise the application to better serve users' requirements, we conducted a detailed co-creation session aimed at discussing the desired features. This session brought together a diverse range of professionals involved in refugee support, including social workers, legal aid experts, and representatives from non-profit organisations.

We then focused on designing and constructing an innovative information-broadcasting system, specifically designed to bridge the communication gap between refugees and assistance organisations. This system facilitates information sharing, enabling more efficient communication between refugees and society.

After constructing the architecture, we carried out an extensive assessment to confirm its effectiveness. This strategy was designed to guarantee data availability with access controls that prioritise the privacy of refugees.

In summary, our research involved an extensive exploration of the information-sharing situation of refugees, leading to the creation and evaluation of IT solutions designed to meet the specific challenges faced by Eritrean refugees in Libya. Through this work, we hope to bridge that gap in communication and social assistance in this area.

## 8.3 Limitations

During the course of this research, several limitations were identified that may have influenced results. One factor to consider is that the insights regarding essential information sharing were derived exclusively from interviews with professionals who are involved in assisting refugees in Libya. This focused approach may limit the applicability of the findings to broader contexts beyond these countries. Therefore, the experiences and insights from these interviews may not fully capture the diverse experiences of refugees from other nationalities, whose aid requirements vary widely.

Moreover, the research was conducted within a specific time frame and geographic scope, which may further limit the relevance of the findings. It is essential to consider these limitations when addressing the complicated issue of refugee assistance across different contexts.

One drawback of the proposed refugee information exchange system is the difficulty users may encounter when using the SPARQL query language. To address this issue, it's essential to develop methods for automatically generating queries that meet users' information requirements. This process would involve converting their requests into SPARQL format, which would facilitate access to the personal information needed for delivering assistance. Large Language Models (LLMs) could play a valuable role in helping to create simple queries. Another factor to consider is how to implement the suggested solution, as it would require an organisation to modify and integrate it into their existing information system.

The challenges we face highlight the necessity for further improvement of the existing system. Continual improvement and innovation will be essential to ensure effectiveness and reliability in the future.

## 8.4 Future Work

To build on these achievements and address existing gaps, future efforts should focus on implementing technical solutions and providing training and resources. Thus, we can create a more effective and secure system that solves the current problem.

- *User Education.* Create comprehensive multilingual training programs designed to educate refugees on the functionality of SOLID data pods, emphasising their importance in maintaining data security and privacy. These initiatives will empower refugees to confidently utilise these technologies, ensuring they understand the principles of data protection and how to manage their personal information safely.
- *Trust-Building Measures.* To effectively demonstrate system reliability, it is essential to showcase example projects and gather feedback from users. Additionally, keeping transparent communication regarding security features will help build trust among potential users, ensuring they feel secure about the system.
- *Interface Optimization.* Design intuitive user interfaces. By incorporating visual assistance such as icons and infographics, along with step-by-step guides, users can navigate the system more seamlessly. This approach ensures accessibility, enhances usability, and fosters interactions.
- *Dashboard Deployment.* The current system is hosted by local servers provided by Inrupt and Streamlit; thus, to use it, one should run the scripts on an Application Programming Interface (API) first. This is challenging for users without technical backgrounds and requires them to read a long document about the environment setup. In future deployments, it's necessary to have the dashboards hosted by a cloud service, so that users can easily access the system via a clickable hyperlink.

By addressing these crucial areas, the SOLID project can develop a secure, user-centric solution that empowers refugees to manage their personal data with confidence and autonomy. This approach not only enhances their privacy but also enables them to control their information, fostering trust and improving their overall digital experience.

Lastly, in this chapter, we summarised the whole research process, from identifying the problem to system evaluation. By analysing the work we've done, a clearer picture of the future work was drawn.

# 9 Conclusion

In this concluding chapter, we will provide a comprehensive summary of the key findings of our study, exploring how they relate to the initial research objectives and questions. We will also discuss the implications of these findings and how they contribute to our understanding of the topic, paving the way for future research.

In this research, it was identified what the current information sharing situation is for Eritrean refugees in Libya:

- Proper databases are lacking.
- Documents are on paper.
- Digital platforms are absent.
- There is a need for data security.
- Identity issue exists.
- Refugee may distrust digital tools.

Refugees face communication barriers that restrict their ability to contact humanitarian organisations. Moreover, the absence of information technology, like smartphones and internet access, makes it harder for them to connect with support institutions that could assist them.

After understanding the problems and their importance, it was essential to create a solution. In this thesis, we propose a comprehensive information-sharing system designed specifically to empower refugees, particularly those from Eritrea. The system consists of a SOLID-based platform that enables refugees to effectively share their specific needs. Additionally, we incorporate a Query Assistant utilising SPARQL, enabling organisations to query and analyse the data collected easily. The refugee information is stored in SOLID data pods, formatted in RDF, which facilitates querying that can extract critical insights and generate knowledge graphs. This innovative platform acts as a vital resource to help tackle the challenges faced by Eritrean refugees.

Moreover, data privacy is carefully preserved by implementing access control policies and techniques. Our system emphasises user privacy by adhering to SOLID protocols for managing personal data. Furthermore, transparency is ensured by allowing refugees to revoke consent and limit access to their personal information. As a result, our system is designed to improve the efficiency and effectiveness of information sharing for refugees. This research provides support for Eritrean refugees in Libya who may encounter difficulties in communicating their needs to humanitarian organisations.

In conclusion, this research aims to provide a communication system for Eritrean refugees in Libya. We first identified the existing problems in the information sharing for refugees through interviews and a co-creation session. The gathered requirements were then transformed into system functionalities, and a system architecture was proposed. Implementation details of the system and example user flow were explained. A thorough evaluation was conducted from both technical and user testing aspects.

# Bibliography


[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 protect
newline on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Consolidated text (OJL119, 04.05.2016; corrigendum OJL127, 23.05.2018).

[2] Ademola Abass. Historical and political background to the malabo protocol. *The African Criminal Court: A Commentary on the Malabo Protocol*, pages 11–28, 2017.

[3] Ayat Ayman Abdel-Aziz, Hassan Abdel-Salam, and Zeyad El-Sayad. The role of icts in creating the new social public place of the digital era. *Alexandria Engineering Journal*, 55(1):487–493, 2016.

[4] Oyeniyi Abe and Ada Ordor. Addressing human rights concerns in the extractive resource industry in sub-saharan africa using the lens of article 46 (c) of the malabo protocol. *Law and Development Review*, 11(2):843–878, 2018.

[5] Rene Abraham, Johannes Schneider, and Jan Vom Brocke. Data governance: A conceptual framework, structured review, and research agenda. *International journal of information management*, 49:424–438, 2019.

[6] ACAPS. Italy Central Mediterranean route: Overview. `https://www.acaps.org/country/italy/crisis/central-mediterranean-route`, February 2022. Web Page, 23 February 2022.

[7] African Union. African union convention on cyber security and personal data protection. `https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf`, June 2014. Adopted in Malabo, Equatorial Guinea, 27 June 2014. Treaty No. 0048.

[8] Ibrahim Alhassan, David Sammon, and Mary Daly. Data governance activities: an analysis of the literature. *Journal of Decision Systems*, 25(sup1):64–75, 2016.

[9] Grigoris Antoniou and Frank Van Harmelen. *A semantic web primer*. MIT press, 2004.

[10] Marcelo Arenas, Claudio Gutierrez, and Jorge Pérez. Foundations of rdf databases. In *Reasoning Web International Summer School*, pages 158–204. Springer, 2009.

[11] Felicity G Attard. *The duty of the shipmaster to render assistance at sea under international law*, volume 41. Brill, 2020.

[12] Assefaw Bariagaber. Globalization, imitation behavior, and refugees from eritrea. *Africa Today*, 60(2):3–18, 2013.

[13] Kyle Beadle. The possibilities of data resistance in a digital society. British Academy, 2024.

[14] Tim Berners-Lee. Linked data. `https://www.w3.org/DesignIssues/LinkedData.html`, 2006. Accessed: 2025-05-20.

[15] Tim Berners-Lee, Yuhsin Chen, Lydia Chilton, Dan Connolly, Ruth Dhanaraj, James Hollenbach, Adam Lerer, and David Sheets. Tabulator: Exploring and analyzing linked data on the semantic web. In *Proceedings of the 3rd international semantic web user interaction workshop*, volume 2006, page 159. Athens, Georgia, 2006.

[16] Tim Berners-Lee, Roy Fielding, and Larry Masinter. Uniform resource identifier (uri): Generic syntax. Technical report, 2005.

[17] Balázs Bodó, Jaya Klara Brekke, and Jaap-Henk Hoepman. Decentralisation: A multidisciplinary perspective. *Internet Policy Review*, 10(2):1–21, 2021.

[18] Stefano Bortoli, Themis Palpanas, and Paolo Bouquet. Decentralised social network management. *International Journal of Web Based Communities*, 7(3):276–297, 2011.

[19] Dan Bouhnik and Yahel Giat. Information gatekeepers–aren't we all? *Informing Science*, 18:127, 2015.

[20] Jorge Cardoso and Amit Sheth. The semantic web and its applications. In *Semantic Web Services, Processes and Applications*, pages 3–33. Springer, 2006.

[21] Stephanie Russo Carroll, Ibrahim Garba, Oscar L Figueroa-Rodr´iguez, Jarita Holbrook, Raymond Lovett, Simeon Materechera, Mark Parsons, Kay Raseroka, Desi Rodriguez-Lonebear, Robyn Rowe, et al. The care principles for indigenous data governance. *Open Scholarship Press Curated Volumes: Policy*, 2023.

[22] Peter Chonka and Yidnekachew Haile. Information and communication technologies and mobility in the horn of africa. *London: EU Trust Fund for Africa (Horn of Africa Window) Research and Evidence Facility*, 2020.

[23] Sara Creta. Active agency, access and power: Social media and eritrean refugees in libya. *Enslaved Trapped and Trafficked in Digital Black Holes: Human Trafficking Trajectories to Libya*, pages 759–785, 2023.

[24] Azadeh Dastyari and Asher Hirsch. The ring of steel: Extraterritorial migration controls in indonesia and libya and the complicity of australia and italy. *Human Rights Law Review*, 19(3):435–465, 2019.

[25] Stefan Decker, Sergey Melnik, Frank Van Harmelen, Dieter Fensel, Michel Klein, Jeen Broekstra, Michael Erdmann, and Ian Horrocks. The semantic web: The roles of xml and rdf. *IEEE Internet computing*, 4(5):63–73, 2000.

[26] Stefan Decker, Prasenjit Mitra, and Sergey Melnik. Framework for the semantic web: an rdf tutorial. *IEEE Internet Computing*, 4(6):68–73, 2000.

[27] Ruben Dedecker, Wout Slabbinck, Jesse Wright, Patrick Hochstenbach, Pieter Colpaert, and Ruben Verborgh. What's in a pod? a knowledge graph interpretation for the solid ecosystem. In *6th Workshop on Storing, Querying and Benchmarking Knowledge Graphs (QuWeDa) at ISWC 2022*, volume 3279, pages 81–96. CEUR, 2022.

[28] Hugh Dubberly and L Sanders. An evolving map of design practice and design research. *Research Quarterly*, 1:13–17, 2006.

[29] Bob DuCharme. *Learning SPARQL: querying and updating with SPARQL 1.1*. " O'Reilly Media, Inc.", 2013.

[30] First Nations Information Governance Centre (FNIGC). OCAP®Principles  Best Practices Fact Sheet, December 2022. Published by University of Ottawa Library; English version (final).

[31] Médecins Sans Frontières. Trading in suffering: detention, exploitation and abuse in libya. *Médecins Sans Frontières*, 2019.

[32] Christian Fuchs and Eva Horak. Africa and the digital divide. *Telematics and informatics*, 25(2):99–116, 2008.

[33] TG Gebreslassie, Gebru Kidanu, Liya Mamo, SY Amare, and Mirjam Van Reisen. Life in darkness: The communication blockade during the tigray siege. *Tigray. War in a Digital Black Hole, Book*, 3, 2024.

[34] Global Indigenous Data Alliance (GIDA). CARE Principles for Indigenous Data Governance, January 2019. Accessed from GIDA website; first drafted at a workshop on 8 November 2018 in Gaborone, Botswana.

[35] Tom Heath and Christian Bizer. *Linked data: Evolving the web into a global data space*. Morgan & Claypool Publishers, 2011.

[36] Antonio Hernández-Illera, Miguel A Mart´inez-Prieto, and Javier D Fernández. Rdf-tr: Exploiting structural redundancies to boost rdf compression. *Information Sciences*, 508:234–259, 2020.

[37] Betina Hollstein. Qualitative approaches. *The SAGE handbook of social network analysis*, 1(01):404–416, 2011.

[38] Christopher Horwood and Kate Hooper. Protection on the move: Eritrean refugee flows through the greater horn of africa. *Transatlantic Council on Migration, 1*, 29, 2016.

[39] Human Rights Council. Report of the detailed findings of the commission of inquiry on human rights in eritrea. `https://digitallibrary.un.org/record/798731`, 2015. UN Document A/HRC/29/CRP.1.

[40] Patrik Hummel, Matthias Braun, Max Tretter, and Peter Dabrock. Data sovereignty: A review. *Big Data & Society*, 8(1):2053951720982012, 2021.

[41] Amnesty International. Libya's dark web of collusion: Abuses against europe-bound refugees and migrants, 2017.

[42] Amnesty International. 'between life and death'. refugees and migrants trapped in libya's cycle of abuse., 2020.

[43] Maanpreet Kaur. The criminalisation of ngo-led sar operations: A contributing factor towards crimes against humanity against migrants in libya, 2023.

[44] Navin Keizer, Onur Ascigil, Michal Król, Dirk Kutscher, and George Pavlou. A survey on content retrieval on the decentralised web. *ACM Computing Surveys*, 56(8):1–39, 2024.

[45] Katie Kuschminder and Anna Triandafyllidou. Smuggling, trafficking, and extortion: New conceptual and policy challenges on the libyan route to europe. *Antipode*, 52(1):206–226, 2020.

[46] Clément Labadie and Christine Legner. Understanding data protection regulations from a data management perspective: a capability-based approach to eu-gdpr. In *Proceedings of the 14th International Conference on Wirtschaftsinformatik (2019)*, 2019.

[47] He Li, Lu Yu, and Wu He. The impact of gdpr on global technology development, 2019.

[48] Lawless Libya. Mirjam van reisen, klara smits & morgane wirtz. *Mobile Africa: Human trafficking and the digital divide*, page 261, 2019.

[49] Essam Mansour, Andrei Vlad Sambra, Sandro Hawke, Maged Zereba, Sarven Capadisli, Abdurrahman Ghanem, Ashraf Aboulnaga, and Tim Berners-Lee. A demonstration of the solid platform for social web applications. In *Proceedings of the 25th international conference companion on world wide web*, pages 223–226, 2016.

[50] Daniel Rezene Mekonnen and Meron Estefanos. From sawa to the sinai desert: The eritrean tragedy of human trafficking. *Available at SSRN 2055303*, 2011.

[51] UN OCHA. Ethiopia-tigray region humanitarian update situation report. *ReliefWeb, July*, 19:2021, 2021.

[52] Jorge Pérez, Marcelo Arenas, and Claudio Gutierrez. Semantics and complexity of sparql. In *International semantic web conference*, pages 30–43. Springer, 2006.

[53] Martin Plaut. *Understanding Eritrea: Inside Africa's Most Repressive State*. Oxford University Press, 2017.

[54] Ruduan Plug, Yan Liang, Aliya Aktau, Mariam Basajja, Francisca Oladipo, and Mirjam van Reisen. Terminology for a fair framework for the virus outbreak data network-africa. *Data Intelligence*, 4(4):698–723, 2022.

[55] Shelley Powers. *Practical RDF: solving problems with the resource description framework*. " O'Reilly Media, Inc.", 2003.

[56] Keith F Punch. Quantitative and qualitative approaches. *The Sociology of Healthcare: A Reader for Health Professionals*, 51, 2008.

[57] Aravindh Raman, Sagar Joglekar, Emiliano De Cristofaro, Nishanth Sastry, and Gareth Tyson. Challenges in the decentralised web: The mastodon case. In *Proceedings of the internet measurement conference*, pages 217–229, 2019.

[58] Protection Regulation. General data protection regulation. *Intouch*, 25:1–5, 2018.

[59] Mirjam Reisen, Munyaradzi Mawere, Kai Smits, and Morgane Wirtz. *Human Trafficking for Ransom in Black Holes in the Digital Landscape: An Introduction*, pages 1–29. 01 2023.

[60] CRJJ Rijken and MEH van Reisen. Sinai trafficking: Origin and definition of a new form of human trafficking. *Social Inclusion*, 3(1):113–124, 2015.

[61] Andrei Vlad Sambra, Essam Mansour, Sandro Hawke, Maged Zereba, Nicola Greco, Abdurrahman Ghanem, Dmitri Zagidulin, Ashraf Aboulnaga, and Tim Berners-Lee. Solid: a platform for decentralized social applications based on linked data. *MIT CSAIL & Qatar Computing Research Institute, Tech. Rep.*, 2016, 2016.

[62] Luis Sánchez-Fernández and Norberto Fernández-Garc´ia. The semantic web: Fundamentals and a brief state-of-the-art. *Call for Take up Actions, Joined sub-Projects to AXMEDIS project of the European Commission*, 6(6):5–11, 2005.

[63] Oreste Signore. W3c technologies: a key for interoperability. *Journal of Computer Resource Management (a Publication of the Computer Measurement Group, Inc.)*, (110):19–40, 2003.

[64] Shubhadeep D Sinha, Sreenivasa Chary Sriramadasu, Ruby Raphael, and Sudeshna Roy. Decentralisation in clinical trials and patient centricity: benefits and challenges. *Pharmaceutical Medicine*, 38(2):109–120, 2024.

[65] C Matthew Snipp. What does data sovereignty imply: What does it look like. *Indigenous data sovereignty: Toward an agenda*, pages 39–55, 2016.

[66] Colin Tankard. What the gdpr means for businesses. *Network Security*, 2016(6):5–8, 2016.

[67] United Nations Human Rights Office. Libya: Urgent action needed to remedy deteriorating human rights situation – un experts. `https://www.ohchr.org/en/press-releases/2023/03/libya-urgent-action-needed-remedy-deteriorating-human-rights-situation-un`, March 2023. Press release, 27 March 2023.

[68] MEH Van Reisen, Meron Estefanos, and Cornelia Rosalia Jacoba Johanna Rijken. *Human trafficking in the Sinai: Refugees between life and death.* Wolf Legal Publishers (WLP), 2012.

[69] Mirjam Van Reisen. *Enslaved: Trapped and trafficked in digital black holes.* African Books Collective, 2023.

[70] Mirjam Van Reisen, Zecarias Gerrima, Eyob Ghilazghy, Selam Kidane, Conny Rijken, and Gertjan Van Stam. Tracing the emergence of ict-enabled human trafficking for ransom. In *Routledge handbook of human trafficking*, pages 146–156. Routledge, 2017.

[71] Mirjam Van Reisen and Munyaradzi Mawere. *Human trafficking and trauma in the digital era: The ongoing tragedy of the trade in refugees from Eritrea*. African Books Collective, 2017.

[72] Mirjam Van Reisen, Munyaradzi Mawere, Mia Stokmans, Primrose Nakazibwe, Gertjan Van Stam, and Antony Otieno Ong'ayo. Black holes in the global digital landscape: The fuelling of human trafficking on the african continent. *Mobile Africa: Human Trafficking and the Digital Divide. Bamenda, Cameroon: Langaa RPCIG*, 2019.

[73] Mirjam Van Reisen, K. Smits, Mia Stokmans, and Munyaradzi Mawere. The (un)intended role of gatekeepers of information in human trafficking in the digital era, 2020. ZAK Occasional Papers.

[74] Mirjam Van Reisen, Klara Smits, Morgane Wirtz, and Anouk Smeets. Living in a black hole: Explaining human trafficking for ransom in migration. *Enslaved, January*, pages 30–69, 2023.

[75] Paul Voigt and Axel Von dem Bussche. The eu general data protection regulation (gdpr). *A practical guide, 1st ed., Cham: Springer International Publishing*, 10(3152676):10–5555, 2017.

[76] Franziska von Scherenberg, Malte Hellmeier, and Boris Otto. Data sovereignty in information systems. *Electronic Markets*, 34(1):15, 2024.

[77] Morgane Wirtz and Mirjam Van Reisen. Hell on earth: Conditions of eritrean refugees in official detention centres in libya. *Trapped and Trafficked in Digital Black Holes: Human Trafficking Trajectories to Libya. Langaa RPCIG*, pages 570–626, 2023.

[78] Morgane Wirtz and Mirjam Van Reisen. Living skeletons: The spread of human trafficking for ransom to libya. *Enslaved Trapped and Trafficked in Digital Black Holes: Human Trafficking Trajectories to Libya. Bamenda, Cameroon: Langaa RPCIG*, pages 521–569, 2023.

[79] Marcin Wylot, Manfred Hauswirth, Philippe Cudré-Mauroux, and Sherif Sakr. Rdf data storage and query processing schemes: A survey. *ACM Computing Surveys (CSUR)*, 51(4):1–36, 2018.

[80] Kinfe Yilma. African union's data policy framework and data protection in africa. *Journal of Data Protection & Privacy*, 5(3):209–215, 2022.

# Appendices

## A Appendix 1

# B Appendix 2