Universiteit Leiden

Master Computer Science

Emergency Diary: My Secure Data Place - A Decentralised System for Refugee Controlled Emergency Data Management

Name:	Karan Gupta
Student ID:	s4021711
Date:	March 3, 2026
Specialisation:	Data Science
First supervisor:	Dr. Mirjam van Reisen
Second supervisor:	Dr. Lu Cao

Master's Thesis in Computer Science

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

Acknowledgements

I would like to express my sincere gratitude to all individuals and organizations who supported this research.

I am grateful to EEPA (Europe External Programme with Africa), VODAN (Virus Outbreak Data Network) and Sanctuary Foundation for their engagement and support in discussions related to refugee data governance and decentralized infrastructures.

I would like to thank Joëlle Stocker, Daniel Tesfa, and Makeda Saba for their valuable insights and collaboration. Their contributions significantly enriched empirical and contextual grounding of this study.

My sincere appreciation goes to Tangaza University for its support in relation to FAIR Data Point (FDP) and broader discussions on FAIR aligned data infrastructures.

I would further like to thank all members of the DSIP (Data Science in Practice) Fieldlab for their collaboration and engagement during the iterative development of the prototype system: Deepak Somesh K J, Divyanshi Singh, Nallathambi Vethiappan, Ilakiya Sulur Ravi Sumathi, and Krithik Raja Kesavan.

The fieldlab environment provided an important space for discussion, experimentation and technical reflection.

Finally I extend my gratitude to all refugee and NGO participants who generously shared their time and perspectives for this research.

Contents

Chapter 1

Introduction

1.1 Problem Statement

The global refugee crisis has reached unparalleled proportions with more than 110 million people recently forcefully displaced globally. Refugees are exposed to detention, extortion, trafficking, poor living conditions and recurrent violations abuses of human rights. However the mechanisms for documenting and reacting to these experiences are still fragmented and lacking. Refugees frequently lack both the resources and the trust to record their travels in a safe and structured way. The majority of humanitarian databases currently in use are centralised and managed by international organizations offering little transparency or agency to the individuals whose data is being gathered [1, 2]. The literature has referred to this as a crisis of digital agency, in which refugees are compelled to provide sensitive information such as biometric, health information and location without their knowledge or meaningful control over how this data is used [2]. Previous studies contend that digital identity platforms created for refugees usually reinforce bureaucratic control and exclusion rather than empowering displaced individuals [3]. According to further research, women and marginalised groups are especially vulnerable often excluded from decision making around their own data and subject to heightened risks of surveillance or exclusion [1]. From the perspective of humanitarian organisations the absence of structured, refugee focused reporting hinders the ability to spot patterns and respond effectively. Similar events such as ransom demands, checkpoints or disappearances are rarely linked across individuals and remain isolated fragments of information. This fragmentation in reporting make it more tough for humanitarian organisations to retrieve structure information, identify vulnerability patterns or coordinate responses effectively. Scholars have described the humanitarian sector as being impaced by 'data hubris', in which the desire to gather big data (biometrics, crisis mapping and blockchain experiments) surpasses the capacity to analyse it responsibly [4]. this tendancy has led to ethicaly questionable experimentation on vulnerable groups undermining the principle of 'do no harm' [5]. New technology attempts to fill these gaps have often fallen short. For example biometric registration systems have been criticised for putting bureaucratic efficiency and surveillance ahead of protection and empowerment [3, 6]. Blockchaiun based identity solutions though widely promoted remain inaccessible to many refugees who lack digital literacy [7]. Similar to this initiatievs to apply AI or decentralised architectures in refugee contexts have shown promise but are still at the experimental stage raising questions about feasibility and risks of harm [8]. In contrast the decentralised web technologies like solid pods present a much more feasible alternative enabling refugee controlled data management without infrastructural and technical burdens linked with

blockchain systems. The specific problem this thesis tackles or addresses is therefore twofold. First there isn't a secure system that allows refugees themselves to record structured event based data (like date, location, situation, needs etc) while maintaining control over access permissions. Second, NGOs don't have the analytical tools that can group such data into meaningful patterns for example by identifying clusters (patterns) of similar information across individuals. Without these tools both refugee agency and NGO effectiveness remains limited. This study (research) proposed ton address this gap by exploring a refugee centered emergency incident reporting system built around the ideas or principles of informed consent and selective data sharing. Building on the promise os decentralised technologies such as Solid Pods refugees would be able to store their own entries and decide whether NGOs can access them or not [9]. On the NGO's side, this system would offer structured SPARQL based filtering that would allow the NGOs to search records by shared features like location, date ranges, gender, reasons for seeking help etc. This would enable the NGOs to spot patterns of risk and repsond more efficiently while ensuring that refugees retain sovereignty over their data.

In summary the problem this thesis addresses is the absence of a trusted refugee centered mechanism for recording and sharing incident data combined with the lack of analytic methods that allow NGOs to interpret that data in ways that respect privacy and agency. This dual gaps leaves refugees disempowered and NGOs underinformed thereby undermining humanitarian protection. Bridging this gap requires a system that is both technically robust and ethically aligned grounded in the principles of privacy, trust and digital agency [10].

1.2 Synthesis of the Problem Statement

The literature repeatedly demonstrates that displaced populations are caught between two failures: on the one hand refugees are asked to provide highly sensitive personal data into systems they neither trust nor control and on the other hand humanitarian organisations lack trustworthy, structured data to interpret refugee data and coordinate responses [2, 6]. As a result there is a continuous gap where the voices and experiences of refugees remain under documented while NGOs are left with fragmented information that prevents timely and coordinated intervention. At the core of the problem is the imbalance between data usability and data sovereignty. Centralised systems, biometric registration and experimental technologies have tended to prioritise bureaucratic efficiency or innovation over refugee protection often exacerbating risks of exclusion and surveillance [3, 5]. At the same time NGOs struggle to identify meaningful patterns across incidents like repeated ransom demands or detentions at the same location because individual reports are not aggregated into a usable whole [4].
The synthesis of this problem is therefore clear: there is presently no trusted mechanism that allows refugeees to record their experiences with control over consent while also allowing NGOs to detect actionable patterns in the data. Addressing this dual gap required a system that integrated refugee centered data sovereignty with NGO oriented analytical tools ensuring that humanitarian response is both ethical and effective.

1.3 Research Questions

Building on the synthesis of this problemn this thesis is guided by one overaching research question and four interrelated sub questions. Together these questions provide a logical se-

quence from identifying needs, through system specification to deployment and assessment of adoption potential.

Overarching Research Question
How can a refugee centered emergency incident reporting system be designed and implemented to empower refugees with control over their data while enabling NGOs to search, filter and interpret structured patterns in the reported data in a way that is both technologically robust and ethically aligned?

Sub-Questions:

- RQ1: Needs - What are the needs and priorities of both refugees and NGOs in relation to data recording, sharing and analysis?
- RQ2: Specifications and Requirements - What are the functional and non functional specifications required for designing a solid based emergency reporting system that meets these needs while safeguarding privacy, consent and digital agency?
- RQ3: Deployment - How can such a system be implemented and deployed in a technically feasible manner that meets the identified specifications?
- RQ4: Adoption potential - What is the potential for adoption of this system by refugees and NGOs considering usability, trust and ethical acceptability?

These research questions align with the methodological steps of the thesis which are conducting a literature review, examining the needs of refugees and NGOs via interviews, translating those needs into specifications, developing and deploying a prototype and finally assessing the potential for adoption in real world humanitarian context.

1.4 Research Objectives

The motive of this study is to design, implement and evaluate a refugee centered emergency data reporting system that balances the dual needs of refugees and NGOs ensuring both data sovereignty and actionable insights. To achieve this motive the following objectives are formualated:

- Objective 1: Identify Needs (RQ1) - The first objective is to identify the needs and priorities of both refugees and NGOs with regards to recording, shairing and analysing incident related data. Refugees require a safe , trustworthy mechanism to document their emergency information in a controlled and secured manner without fear of surveillance or misuse while NGOs require structured and reliable data to identify patterns and respond effectively.
- Objective 2: Define Specifications (RQ2) - The second objective is to translate the identified needs into funcitonal and non functional specifications for an emergency data reporting system. These specifications will outline the features required like structured data entry, consent management and SPARQL based data querying as well as non funcitonal requirements like security, privacy and usability. This step ensures that system

is not only technically viable but also ethically aligned with the principle of refugee agency and humanitarian accountability.

- Objective 3: Prototype Implementation (RQ3) - The third objective is to design and implement a prototype that embodies the specifications. The prototype will allow refugees to create structured emergency incident records, control access to their data and optionally share information with the NGOs. On the NGO side the system will include a structured SPARQL based filtering that groups comparable entries to reveal patterns.
- Objective 4: Adoption Potential (RQ4) - The fourth objective is to assess the adoption potential of the system among the refugees and whewther the NGOs find the outputs meaningful for their work. Beyond technical performance this evaluation will consider ethical acceptability and practical feasibility ensuring that the system is not only innovative in theory but also relevant and implementable in practice.

Together these objectives provide a structured pathway from problem identification through design and implementation ensuring that the research is both theoretically grounded and practically relevant.

1.5 Relevance

1.5.1 Academic Relevance

This study is relevant to ongoing discussions in information systems, humanitarian technology and digital identity studies. Scholars have emphasised ongoing concerns about the the erosion of refugee agency in digital identity systems and the ethical risks of humanitarian data practices [2, 3, 6]. At the same time the literature points to a lack of empirical systems that practicaly reconcile the dual demands of protecting individual data rights and enabling organizational effectiveness [4, 5]. By creating and evaluating a prototype that explicitly prioritises refugee control (through consent mechanisms) while providing NGOs with useful insigths (through structured querying) this research contributes a concrete model that bridges theoretical frameworks with technical implementation. It also enhances the discussion on decentralised strategies such as Solid and Personal data stores which are only beginning to be studied in migration and humanitarian contexts [8, 9].

1.5.2 Societal Relevance

The societal relevance of this research is immediate and pressing. With more than 110 million people forcibly displaced worldwide the humaitarian sector faces urgent challenges in protecting and assisting refugees. Current information systems often fail to capture refugee voices securely resulting in missed opportunities to detect patterns of abuse, respond to crises and protect vulnerable groups [1]. At the same time refugees often mistrust centralised data collection practices as these frequently expose them to surveillance and exclusion rather than empowerment [2]. By creating a refugee centered emergency information reporting system this project addresses both sides of the problem. It offers refugees a trusted, consent based way to record their experiences and it provides NGOs with structured, queryable data that can enhance humanitarian response. In the current scenario of increasing displacement the ability to balance ethical data practices with actionable insights is critical not only for immediate

humanitarian interventions but also for long term policy and protection frameworks.

In summary this research is relevant as it tackles a pressing societal need while addressing an academic gap. It contributes to the scholarly debate on digital identity, data justice and humanitarian technology while at the same time proposing a practical solution with the potential to improve the protection and dignity of refugees in real world contexts.

1.6 Location

This study sits at the intersection of refugee protection, humanitarian studies and information systems design. Conceptually, it belongs to the domain of digital identity and humanitarian data management where questions of privacy, consent and ethical use of information are central [2, 3]. Geographicaly the focus of this study is on Eritrea and other African countries that experience high levels of forced migration and displacement. Eritrea has been a major country of origin for refuees due to ongoing political repression, mandatory national service and human right violations. Many Eritrean refugees flee through dangerous migration routes across Sudan, Ethiopia, Libya and the Mediterranean where they ared exposed to detention, ransom demands, trafficking and loss of family members. These challenges are not unique to Eritrea but resonates across multiple African contexts where refugees encounter similar patterns patterns of risk, exploitation and limited access to secure data systems. By situating the research in this regional context the study directly addresses the urgent need for systems that can both protect refugee data and provide NGOs with the insights necessary to respond efficiently. Practically the prototype is develope and assessed within an academic research environment but the design is informed by literature, reports and case studies on African refugee experiences [1, 5]. This ensures while the work doesn't involve direct fieldwork with vulnerable populations it remains grounded in the realities faced by refugees. The system is therefore conceived as both a response to the specific needs of African refugee contexts and as a model that could be adopted for use in other displacement settings globally.

1.7 Contextual Background: Eritrean Refugees

Eritrean refugees constitute a very big and protracted refugee population in East Africa. Many Eritrean flee indefinite national service, political repression, human rights concern as a result of which many Eritrean refugee communities are hosted in neighbouring countries like Ethiopia and Kenya.

Eritrean refugees constantly engage with humanitarian organizations , NGOs and government agency for documentation, protection service, food help and resettlement procedure. These interactions often require repeated disclosure of sensitive personal information across multiple systems. Refugees in such context may experience structural vulnerabilities including power imbalance in institutional interactions, limited control over personal data and concern about misuse of information. Trust in institutions is thus shaped by both past experience in country of origin and by governance practices in host countries.

1.8 Ethical Considerations

Working with refugee related data and designing systems for humanitarian use require careful attention to ethics. Refugees are among the most vulnerable population often exposed to surveillance, exploitation and political persecution. Any research involving their data even at the design and prototype stage must thus be guided by strong ethical principles.
A first ethical consideration is informed consent. Refugees should never be compelled to share information without clear understanding of how it will be used. The proposed emergency information reporting system is built on the principle of voluntary and selective consent where each entry is private by default and refugees can decide whether to share it with NGOs. Additionally the system records each NGO data view in the refugee's pod enabling full transparency and ensuring that refugees are always aware of when their informstion has been accessed. This design aligns with exisitng calls for respecting refugee digital agency and avoiding one sided data collection practices [1, 2].
A second consideration is privacy and data protection. Previous studies have documented the risks of centralised humanitarian databases and biometric systems that expose refugees to surveillance or exclusion [3, 6]. To mitigate these risks this research emphasised consent based sharing. Even though the prototype is developed in an academic setting the architecture is designed with security and privacy safeguards that could translate in field use.
A third ethical dimension is the princciple of do no harm. Humanitarian technology initiatives have sometimes been criticised for experimental approaches that prioritise innovation over safety resulting in unintended harm to displace communities [5]. To avoid such pitfalls this research deliberately does not involve direct fieldwork with refugees. Instead it relies on literature, case studies and ethicaln design frameworks to inform development.
Finally there are ethical considerations of representation and relevance. By focusing on Eritrean and other African refugee experiences the research seeks to address real and urgent needs. At the same time it acknowledges the limits of academic research without direct refugee participation. Therefore the findings and prototype are framed as contributions to ongoing dialogue.

In summary the ethical stance of this research is to respect refugee agency, minimise risks and avoid harm. Privacy, consent and security are treated as foundational design requirements rather than optional features. This ensures that the research doesnt reproduce the problematic practices of past humanitarian data initiatives but instead models an approach that is both ethically sound and practicaly relevant.

1.9 Theoretical Framework

This research is based on set of complementing theoretical viewpoints which together tell how digital systems for refugees and humanitarian contexts are understood and analyzed. The theoretical framework sets key assumption about agency, power, trust and data governance which underpin the study.

First the study draws on digital identity in humanitarian and refugee context which stress that identity systems are sociotechnical arrangements shaped by institutional priorities, governance structures etc. Existing literature shows that digital identity system could enable both access to services and at the same time introduce new ways of exclusion, surveillance particularly when refugees have very less control over how their data is collected or used [2, 3, 6].

Second the framework is informed by theory of data justice, data agency which stress questions relating who benefits from data practices and who suffers their risks. Here agency is understood as ability of individuals to meaningfully influence decisions about their personal data instead of complying with externally imposed data requirements. In refugee setting data justice viewpoints draw focus to structural inequalities which define how data is produced, interpreted or acted upon and also to the ways in which vulnerable groups are included from decision making processes surrounding data governance [6, 10].

Third the study deals with literature on humanitarian data practices and ethical risk involving analysis of data collection, experimentation and data hubris. This literature questions assumption that increased data collection necessarily lead to better humanitarian outcome and instead stress the potential for harm when system are deployed without enough contextual awareness or ethical safeguards [4, 5].

Finally the framework includes viewpoints on trust, consent and data governance including principals like FAIR, CARE which talk about the conditions under which data practices may be seen as legitimate and acceptable. According to this viewpoint trust is treated as an output of transparent, participatory data practice. Consent is similarly seen as ongoing process based on power relations and institutional constraints instead of a one time technical formality [3, 9].

Data sovereignty intersects with wider humanitarian debates about dignity and protection. Scholars warn against what has been called 'data hubris' in humanitarian action where large scale data is pursued without sufficient regard for ethics/consequences [4]. CARE [11] directly addresses this critiques and gives a lens via which humanitarian practices could be evaluated.

In addition the framework includes viewpoints from technology adoption theory mainly the Unified Theory of Acceptance and Use of Technology (UTAUT) [12] and Roger's Diffusion of Innovations [13]. These give assumptions about how individuals and organizations evaluate, accept or resist new digital system.

Together these perspectives set a conceptual lens via which digital identity systems and data practices could be examined. They set the study's focus on agency, justice, trust and ethical responsibility. Chapter 2 builds on this framework by reviewing these bodies of literature in greater depth providing the theoretical foundation for further chapters.

1.10 Research Design

The research design refers to the overarching strategy which guide how a study is organized so as to answer its research questions. It define the logic via which data is generated, analyzed and interpreted and tells the relationship between research questions, methods used. Different research designs are suited for different types of research problems depending on whether aim is explanation, exploration, evaluation or creation of artefacts.

A variety of research designs are there including experimental designs, survey based research, case studies, participatory research and design oriented approaches. Each design imply different

assumptions about the nature of evidence and form of research outcomes. Experimental and survey designs are usually used to test hypotheses or measure predefined variables whereas qualitative and design oriented approaches are more useful for exploring complex, context dependent and sociotechnical problems.

The research problem in this thesis concerns the design of digital system for emergency incident reporting in humanitarian and refugee context. This problem is sociotechnical involving issues of agency, trust, consent, data protection and ethical responsibility in addition to technical feasibility. The study aims to explore stakeholder needs, translate these needs into system requirements and develop a solution that respond to real world constraints. For this the research adopts a qualitative, design oriented research approach.

Design oriented research focuses on systematic investigation of problems via the creation and evaluation of artefacts while generating knowledge about the problem and design process itself. Design research is understood as one of several possible research designs instead of a synonym for research design in general. Design oriented research is particularly suited to studies in information systems where the objective is to address practical problems via iterative design and informed by theory and empirical insights [14, 15].

Also this study builds on principals from participatory design which stress the involvement of stakeholders in the research and design process mainly in context where power imbalances and ethical concerns are main. Participatory approaches are commonly employed in humanitarian and community based research to guarantee that systems are responsive to the lived experiences, priorities and concerns of affected populations [10].

This study focuses specially on Eritrean refugees. The selection of this reflect vulnerabilities linked with Eritrean displacements including exposure to trafficking, detention and prolonged migration routes. It was also shaped by feasibility of stakeholder access via academic and humanitarian networks connected to research context. The agenda is not statistical generalisation to all refugee populations but instead an in depth, context sensitive exploration of refugee centered data sovereignty and emergency reporting practices within a defined humanitarian setting.

1.11 Methodology

This study was carried out between September 2025 and February 2026 as part of masters thesis at Leiden University (Leiden Institute of Advanced Computer Science) in the Netherlands. The empirical research focused on Eritrean refugees and NGO representatives involved in refugee protection context.

The methodology of this research is designed to align closely with the four research questions and objectives and to support a depth understanding of refugee centered data practices in humanitarian contexts. At an overview level the study follows a qualitative research methodology combining literature review with empirical data collection and analysis to explore the needs, practices and constraints experienced by refugees and humanitarian organizations in relation to data recording, sharing and use.

Data is collected via multiple qualitative methods like semi structured interviews with relevant stakeholders, focus group discussion and participatory engagement with the Fiedldlab under the course 'Data Science in Practice'. These allow the study to capture diverse viewpoints, lived experiences and organisational practices.

Access to participants was facilitated via academic networks. Two NGO representatives were contacted via the help of first thesis supervisor. Both NGO interviews were carried out in English on zoom application. The first NGO representative Ms. Makeda Saba (Co-Founder of Sanctuary Foundation NGO, Kenya) arranged contact with one refugee participant who was interviewed directly in english on zoom. The second NGO representative Mr. Danial Zemschal Tesfahans (Lecturer and Researcher at Aksum Univeristy, Ethiopia) organized interviews with four refugee participants. These interviews were conducted individually one by one on zoom with the NGO representative present as a translator. As the four participant didnt speak english the discussion was carried out in Tigrinya with real time translation into english by the NGO representative.

A structured questionnaire guide was prepared in advance to guarantee consistency across interviews while allowing flexibility for follow up questions. All interviews were semi structured and audio recorded with individual consent of each participant. Notes were taken during interviews to support analysis later.

The study generated multiple form of qualitative data:

- Narrative data from semi structured interviews with refugees and NGO representatives.
- Observational notes from participatory fieldlab sessions and focus group discussions.
- Design artefacts including the prototype, access control configurations etc.

Following data collection interview notes and transcripts were systemized in structured excel sheets to support coding and cross case comparison. The analysis followed a thematic approach involving familarization with data, open coding of recurring concepts, grouping codes into broader thematic categories and comparison between different perspectives. A convergence divergence analysis sheet was developed to systematically spot areas of alignment and tension between stakeholders. The resulting themes were translated into functional and non functional system requirements informing design and implementation of prototype.

The methodological approach adopted in the study is explained in detail in chapter 3 that outlines the research design, data collection methods and analytical procedures. Further chapters build on this methodological foundation by presenting empirical findings, translating identified needs into system specifications and describing the design and evaluation of the prototype.

1.12 Outline of the Thesis

The remainder of this thesis is organised into 8 chapters each addressing a specific stage of the research and corresponding to the research questions.

- Chapter 2: Theoretical Framework - This chapter develops the theoretical foundations of the study in detail. It discusses the concepts of digital agency, data justice, humanitarian information systems and digital identity and explains how these perspectives inform the design and analysis of the research.

- Chapter 3: Methodology - This chapter explains the qualitative methods used to collect and analyse data including literature review, interviews, focus group discussions and participatory engagement with FieldLab.

- Chapter 4: Overview of the Literature Review - This chapter provides a comprehensive review of exisitng literature on refugee data practices, humanitarian technology, digital identity systems and ethical challenges in data driven humanitarian action. The review highlights gaps in current research and situates the present study within this academic discourse.

- Chapter 5: Needs Analysis: Refugee and NGO Requirements - This chapter presents the empirical findings related to the first research question which concerns the needs and priorities of both refugees and NGOs in relation to data sharing and analysis.

- Chapter 6: System Requirements and Design Specifications - This chapter reports on the specifications and requirements of a refugee centered emergency incident reporting system translating the identified needs into concrete design elements and ethical safeguards.

- Chapter 7: System Implementation and Deployment - This chapter describes the development and deployment of the prototype system. It explains how the identified specifications were operationalised and presents the funcitoning of the SPARQL based query engine and consent management features.

- Chapter 8: Adoption Potential - This chapter evaluates the adoption potential of the prototype by considering usability, trust and ethical acceptability and by reflecting on how the system could be applied in real humanitarian contexts.

- Chapter 9: Discussion and Conclusion - The final chapter synthesise the findings from all research questions. It discusses their implications for both theory and practice , reflects on the limitations of the study and offers recommendations for future research and policy.

Chapter 2

Theoretical Framework

2.1 Introduction

The purpose of this chapter is to present the theoretical framework that underpins the study. A theoretical framework provides the conceptual foundation for research by defining and clarifying the main ideas that shape both the research design and interpretation of findings. In the case of this thesis the framework is particularly important as it bring together perspectives from information systems, digital identity studies and humanitarian research to address the double challenge of protecting refugee agency while enabling effective NGO action. The concepts discussed in this chapter involve the principals of SOLID (Social Linked Data) which offers a decentralised model for storage of data and sharing, the FAIR principals which guide data management and operability and RDF which provide the technical language for structuring information. The framework also involves broad socio ethical ideas like data sovereignty which emphasise control and ownership of data, technical adoption that highlights the factors affecting the uptake of new systems and data privacy and legal frameworks that sets the boundaries for ethical and lawful data use. Finally the chapter talks about ethical and humanitarian design principals particularly the idea to 'do no harm' in humanitarian technology.

Together these ideas form the theoretical basis of the thesis. They not just guide the development of the emergency incident information reporting system but also provides criteria for assessing its ethical soundness and potential for adoption.

2.2 SOLID (Social Linked Data)

The first key concept of this study is SOLID (Social Linked Data) an initiative launched by Tim Berners Lee to redecntralise the web and restore individual control over data [16]. It gives a technical architecture in which users stores their data in personal online data stores known as pods rather than relying on centralise platforms. Each pod is controlled by the individual user who can determine which applications/organisations are granted access to resources. This model is built on established web standards particularly RDF and enables data to be linked and shared across different systems without requiring central ownership [9].
A central principal of Solid is fine grained access control. Unlike conventional centralised systems where control is given to service providers SOLID allows individuals to grant or revoke access at the level of individual files. Access decisions are enforced through Web Access Control

(WAC) [17] and Access Control Policies (ACP) [18] ensuring that data use always reflects the consent of the owner. This makes Solid especially relevant for contexts where trust, privacy and sharing are important.
In the humanitarian and refugee context the Solid model addresses a fundamental gap. Refugees are frequently required to give personal and biometric data to multiple organisations without clear control over how this data is stored or reused [2]. By storing entries in personal pods refugees could retain sovereignty over their data choosing whether to keep information private or share it with NGOs. This aligns with the objectives of the emergency incident reporting system proposed in this thesis where each entry is private by default but can be shared with NGOs based on informed consent.
Recent studies have also explored the application of Solid in privacy sensitve domains like healthcare, genomecs and social media showing it's potential to increase user agency and interoperability [8]. These applications give proof of consent that Solid can functions as a backbone for systems where sensitive personal information must both be protected and shared under controlled conditions. Extending these insights to the refugee context offer a promising pathway for addresing the current imbalances between refugee agency and NGO data needs.

2.3 FAIR Principles

Another important idea for this study is the set of FAIR principals which stand for Findable, Accessible, Interoperable and Reusable. Originally formulated on the context of scientific data management the FAIR principals aim to guarantee that data is organised and described in ways that make it usable both by humans and machines [19]. Specifically FAIR emphasises the use of standardised metadata, persitent ideentifiers and open formats to guarantee tht data could be dicsovered, accessed under clear conditions, integrated across systems and reused for future research/applications [19, 20].
The FAIR framework has widely been adopted in field like health, genomics and science where the volume and complexity of data requires systematic approaches to data stewardship and guarantee long term usability [20]. In humanitarian contexts existing study highlight challenges relating to fragmented data infrastructures, limited interoperability between organizations and duplicate data collection efforts all of which could undermine coordination and evidence based decision making [4]
Similarly research about refugee data practice has shown that inadequate data structuring and governance could affect the aggregation and analysis of information needed to spot risks and coordinate intervention [1].
From this point of view the FAIR principals give a conceptual lens for understanding how data might be structured in ways which support analytical use and coordination of organizations while staying compatible with access restriction and protection requirement.

2.4 FAIR-OLR (Ownership, Localisation and Regulatory Compliance) Framework

The FAIR-OLR framework [21] extends original FAIR principals by including three more governance dimensions: Ownership, Localisation and Regulatory Compliance. While FAIR focus on technical qualities of data like findability and interoperability FAIR-OLR address governance

and jurisdictional conditions under which sensitive data is stored, accessed and reused. The FAIR OLR framework emerged from research on federated health data infrastructures specially within VODAN Africa initiative [21]. It suggest for sensitive and personal data FAIR implementation should be grounded in data ownership by data subject, localization of data within jurisdiction where it is produced and compliance with regulatory frameworks.

Ownership: As per the study [21] ownership is a foundational principal from which access and control arrangements are derived. The paper stresses that personal data pertain to data subject and is stewarded by data producer with consent of data subject.

Localisation: Localisation concerns juridictional and structural location of data. The FAIR OLR paper [21] stresses data localization is important if ownership is to be meaningfully held. In VODAN Africa model health data is stored in residence within health facility where it is produced and personal data doesn't leave the jurisdiction.

Regulatory Compliance: Regulatory Compliance refer to adherence to applicable legal frameworks in jurisdiction where data is stored and processed. It recognise that data governance must operate within existing legal obligation and institutional accountability structure. In contexts involving cross border data flow or mobile population this dimension highlight the complexity of determining which regulatory regime apply.

By extending FAIR with these dimensions FAIR-OLR give a framework specially relevant for sensitive domains like health and humanitarian data infrastructures.

2.5 RDF (Resource Description Framework)

The resource description framework (RDF) is a foundational idea/standard of the semantic web and serves as a flexible data model to representing information. RDF was introduced as part of broad vision of Semantic Web which aims to allow data to be shared, linked and reused across applications and orgranizational boundaries [22]. RDF structures data in the form of triples-subject, predicate and object which toegther expresses relationship between entities. This method allows data to be machine readable, semantically explicit and interoperable across different system.
In the context of this study RDF provides a technical foundation for representing refugee incident records in a structured and standardised way. Each incident record can be expressed as a set of RDF triples where attributes such as date, location, condition, specific needs etc are described explicitly. This makes sure that information is not only stored but represented in a format that can consistently be understood by different applications. As a result RDF has been widely talked about as a key enabler of data intergration and reuse on the Web and beyond [23]. RDF also supports extensibiltiy making it possible to include more new attributes or vocab as the needs of refugees and NGOs evolve.
Using RDF is specially valuable in humanitarian contexts where interoperability is vital. NGOs, governments and humanitarian agencies often depend on different systems and databases that can lead to fragmentation and duplication. RDF helps overcome this by offering a shared, standardised model for representation data. In this manner semantic technologies like RDF have been proposed as a means of addressing structural interoperability challenges by allowing

data to be represented in a shared and extensible format which support integration across systems [22, 23].

2.6 Semantic Modelling: Ontologies, Metadata and Controlled Vocabularies

Beyond RDF semantic modelling relies on shared conceptual definitions and controlled representation of meaning.

An ontology provide a formal specification of concepts, classes and relationships within a domain. It define how entities like incidents, locations or need are categorized and related to each other.

Controlled vocabularies refer to predefined list of allowed values for specific attributes. Instead of allowing unrestricted free text input controlled vocabularies constrain entries to standardized terms.

Metadata refer to data about data. Different forms are:

- Syntactic metadata which define structural format and encoding.
- Semantic metadata which clarify meaning and relationship between data elements.
- Content metadata which describe subject matter or substance of the data.

Together RDF, ontologies, metadata structures and controlled vocabularies form semantic infrastructure necessary for machine readability, interoperability and structured analysis.

2.7 Data Sovereignty

The idea of data sovereingity refers to the right of individuals/communities to control the collection, owenership and use of their own data. In contrast to centralised systems where data is extracted and managed by institutions data sovereignty emphasises agency, consent and accountability. It is rooted in broader debates on digital rights and data justice which argues that individuals should not just have access to their data but be also empowered to decide how it is stored, shared and reused.
In refugee contexts data sovereignty is particularly significant because displaced populations are often deprived of it. refugees are frequently asked to give personal and biometric information to governments, internal organisations and NGOs in exchange for access to aid and protection [6]. Once provided this data is frequently stored in centralised databases which refugees cant access or control. Research shows that such systems can amplify vulnerabilities. They may be used for surveillance, shared without consent or even misused by hostile actors [1]. In this manner the absence of data sovereignty deepens the power imbalance between refugees and institutions which govern them.
An important difference within modern debates on data sovereignty is between state centred data sovereignty and community centred data sovereginity. State data sovereignty usually

refers to the authority of governments over data generated within their territorial/legal jurisdiction often stressing national control, regulation and security. On the other hand community centred data sovereignty focuses on collective rights of communities particularly marginalized or exploited groups, to govern data in ways which reflect their values, priorities and interests. This community oriented viewpoint is addressed in the Care principals for Indigenous Data Governance which stand for Collective benefit, Authority of control, Responsibility and Ethics [11]. CARE talks about question of power, justice and governance by stressing that data practices should benefit the communities concerned, respect their authority about data and be guided ethically.

2.8 Technology Adoption

For any technological system to be effective it must not only be designed and implemented but also adopted by its intended users. In the case of this study adoption refers both to refugee's willingness to use the emergency incident reporting system to record and share their experiences and to NGO's willingess to integrate the system into their worklflows for analysis and response. Without adoption on both sides even the most technically robust and ethically designed systems are at the risk of irrelevance.
The academic literature talks about certain models to explain how and why individuals or organisations adopt new technologies. The TAM (Technology Acceptance Model) emphasises 2 key factors- percieved usefullness and perceived ease of use [24]. A system is more likely to be adopted if users believe it will improve their situation and if it is straightforward to use. In the refugee context this means that refugees will will only use the system if it contributes to their safety/dignity and doesnt present additional risks/complexities. Similarly NGOs will only adopt the system if it serves actionable insights that complement/improve upon their existing information systems.
Further research expanded TAM into comprehensive frameworks. Notably the Unified Theory of Acceptance and Use of Technology (UTAUT) involves multiple adoption models and identifies performance expectancy, effort expectancy, social influence and fascilitating conditions as main determinant of adoption [12].
UTAUT [12] offers a structured way to see how different factors affect an individual or organization's willingness to adopt and use a technological system. It conceptualizes adoption as being shaped by various interelated constructs which include perceived usefulness, perceived ease of use, social and organizational influence and the presence of enabling conditions. This all make the framework particularly suitable for analyzing adoption in humanitarian and organizational contexts where decisions to use are shaped by ethical considerations, trust relationships, institutional practices and resource constraints.

The 5 UTAUT constructs are:

- **Performance Expectancy:** It refers to the extent to which stakeholders believe that the system would be beneficial or useful in their context.
- **Effort Expectancy:** It relates to the perceived ease of use and interaction comfort.
- **Social Influence:** It captures the role of opinions, ideas and trust relationships in shaping adoption.

- **Facilitating Conditions:** It refers to extent to which stakeholders believe that necessary technical, organizational support is available to enable use of system.
- **Behavioural Intention:** It reflects expressed willingness or openess to adopting the system.

Each of these constructs is studied in a dedicated section using interview data which relates to adoption considerations.

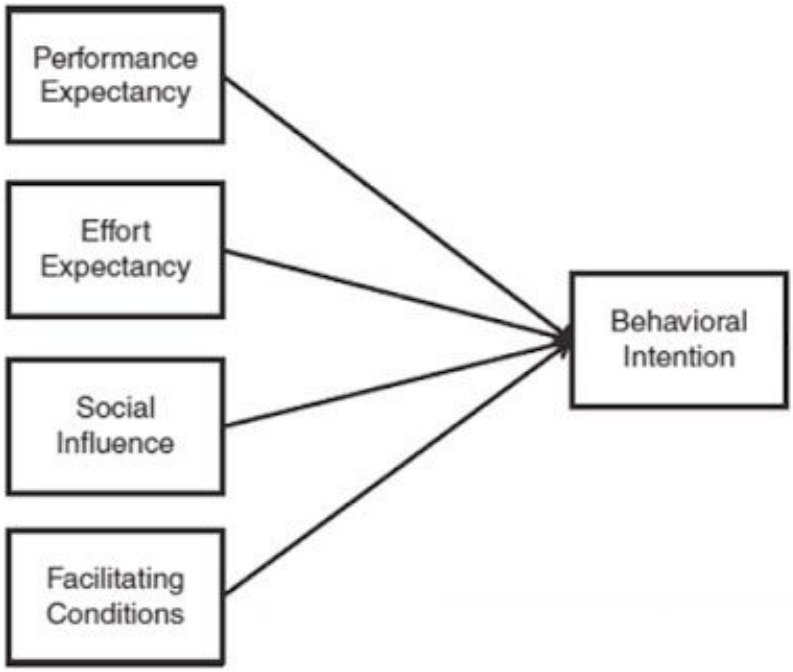


Figure 2.1: UTAUT Framework

The Diffusion of Innovations (DOI) theory provides a complementary perspective highlighting how adoption spreads within a social system [13]. It identifies attributes like relative advantage, compatibility, complexibility and observability as determinants of adoption. Applied here means that the emergency incident reporting system tries to show advantages over current practices, align with the workflows of NGOs and the lived realities of refugees and allow for incremental, low risk experimentation. If refugees/NGOs perceive the system as too complex/misaligned with their needs adoption is likely to fail.
In humanitarian contexts however adoption is shaped by more than technical and functional considerations. Trust, legitimacy and ethicl acceptability are critical. Refugees are not likely to use a system if they fear surveillance, retaliation or misues of their information. NGOs on the other hand face reputational and ethical risks if they adopt systems that could expose vulnerable populations to harm. Research shows that adoption in such contexts depend heavily on assurances of privacy, transparency and alignment with humanitarian prinicipals [5].
In this thesis adoption is thus treated as both a technical challenge and a social process. The evaluation/assessement of the prototype (RQ4) considers not just whether the system is functional but also whether it inspires trust and is seen as a relevant and legitimate by it's stakeholders. Adoption is the ultimate measure of whether the system can move from a conceptual design to a practical tool that enhances refugee protection and humanitarian action.

2.9 Safeguarding Sensitive Data

Refugee related data/information is very sensitive form of personal data. It often involves detail of identity, location, health, family separation or exposure to voilence. If mishandled such information can endanger lives, compromise asylum claims or subject individuals to surveillance and exploitation. Safeguarding sensitive info is thus not just a technical requirement but an ethical obligation in humanitarian practice and research.
Studies has shown that humanitarian databases and identity systems frequently fall short of such obligation. Refugees are often required to give personal and biometric information in turn of access to aid yet they rarely retain meaningful control over how this information is stored/used [2]. Once data is entered into centralised systems it can be shared between agencies or across borders sometimes without refugees' knowledge/consent. This creates significant risks of misuse and undermine trust which in turn discourage participation in digital identity initiatives [8].

Finally safeguarding sensitive data also includes the dimension of trust. Refugees must feel confident that their information is not being exploited or misused and NGOs need assurance that the data they access has been ethically provided. By adopting a private by default and consent based model this research addresses both sides of that trust relationship ensuring that data protection is a foundational design principal and not an after thought [3].

2.10 Humanitarian Ethics

Designing digital system for refugee's context is not just a technical challenge but an ethical responsibility. Refugee often live in uncertain conditions where the misuse of information can have life threatening consequences/outcomes. As such humanitarian ethics must form the priority of any technological intervention.

One of the most important principals is the humanitarian idea to 'do no harm'. It can occur in digital environments via excessive data collections, insufficient consent mechanism, secondary data use or weak governance structures. Past experiences with humanitarian experimentation such as large scale biometric databases or blockchain illustrate how innovation without safeguards can undermine protection goals [4]. These lessons highlight the importance of caution,accountability and risk awareness in system design.

Another ethical consideration is participation and agency. Refugees have often been put in a spot as passive data subjects with little say over how there information is collected or used. Ethical approaches to design stress meaningful agency, transparency and informed decision making recognizing affected population as rights bearing actor instead of just beneficiaries of services.

Trust and dignity are also critical ethical principals. Systems should address power imbalance between institutions and displaced population and guarantee data governance practice align with broader humanitarian values of dignity, protection and fairness.

In summary the ethical framework for this research emphasises avoiding harm, respecting agency and building trust.

2.11 Synthesis

The theoretical framework developed in this chapter brings together a set of technical, social and ethical concepts that collectively shape this study. Each concept contributes a distinct perspective yet together they form an aggregated foundation for understanding and addressing the research problem.

From a technical perspective the principals of SOLID and RDF provide the architectural and representational logic for structuring the refugees incident data. SOLID emphasises decentralised storage and consent based sharing while RDF offers a flexible and standardised model for representing entries as structure information. Complementing these the FAIR principals ensure that once consent is given data can be queried in ways which support disocverabiltity and interoperability without compromising security.

From a rights based perspective the concept of data sovereignty establishes that refugees must remain in control of their own information. This principal directly addresses long standing criticisms of humanitarian databases where refugee have historically been treated as passive data subjects. Including sovereignty oriented approach like privacy by default, explicit consent and data minimisation reflect a shift towards recognizing refugee as rights bearing agent within data governance structures. .

From an adoption perspective the literature on technology uptake stresses that systems are only meaningful if they are trusted and used by their intended stakeholders. Refugees must perceive the system as safe and relevant. While NGOs must find the outputs meaningful and reliable. Adoption theories highlight the importance of trust, ease of use and compatibility with existing practices.

Finally from an ethical viewpoint the principals of humanitarian system design underscore the need to avoid harm, respect agency and uphold dignity. Past humanitarian experiments have shown how technologies can unintentionally increase risks. Ethical safeguards are thus understood as conceptual requirement within humanitarian context.

Taken together these concepts form a coherent framework that integrates technical standards with ethical notions and social realities. This framework provide the analytical lens via which refugee centered data practice and digital system design can be assessed in subsequent chapters.

Chapter 3

Methodology

3.1 Introduction

This chapter presents the research design and methodology used in this study. It's purpose is to tell how the research was carried out, what methods were used to collect and analyze data. Doing this the chapter clarifies the overall study design and provides transparency regarding the research process.

Though this this thesis includes the development of an emergency incident reporting system chapter 3 stresses mainly on the methodological approach via which insights were generated including literature analysis, interviews, participatory engagement and collaborative work.

The research is conducted within a humanitarian and refugee context where ethical sensitivity, stakeholder engagement and context understanding is important. Because of this the study adopts a qualitative, design oriented research approach which combines empirical inquiry with participatory elements. Data was collected via multiple methods including literature review, interviews with refugees and NGOs representatives and active participation in a university based Fiedlab focused on the development of the emergency incident reporting system.

This chapter thus outlines research approach, context in which the study was carried out and methods used to collect and analyze data. By clearly documenting these methodological choices the chapter sets the foundation for interpreting the findings shown in later chapters and shows how the research process aligns with study objectives and sub research questions.

3.2 Research Design and Approach

This work follows a qualitative, design oriented research design situated within a humanitarian context. The study is concerned about understanding needs, practices and constraints around refugee data collection and sharing and exploring how these insights could inform the development of an ethically grounded technical solution.

The research design could be characterized as design study with participatory elements. design oriented research is appropriate when goal is not just to analyze an existing thing but also to explore how new artefacts or systems could be shaped in response to real world needs. In this

study the design activity comes as a means of inquiry: insights gained via engagement with stakeholders inform the conceptualization of system whereas the design process itself helps surface ethical, social and organizational considerations relating to refugee practices of data.

Participation plays an important role in the research design. Instead of treating refugees and humanitarian actors as passive subjects the study engages with them to understand their viewpoints, experiences and concerns. This is reflected in the use of interviews with refugees and NGO representative as well as collaboration with the Fieldlab. These interactions allowed reflection on emerging ideas and helped ensure that research remained grounded in lived realities instead of assumptions.

It is important to also stress that research design should not be confused with design model of the system developed in this thesis. The research design is about how knowledge was generated via literature analysis, interviews, participatory engagement and collaborative work while the system design is about how the emergency incident reporting system is structured and implemented.

Overall this research design supports explanatory approach that is well suited to the complexity and sensitivity of humanitarian data practices. By combining qualitative inquiry with participatory design principals the study is able to address research questions in a way which is empirically informed, ethically attentive and responsive to needs of both refugees and humanitarian organizations.

3.3 Research Context and Setting

This research was carried out within an academic and collaborative setting at the Leiden University closely connected to a FiedLab associated with the course 'Data Science in Practice'. The fieldlab formed part of a educational initiative in which students worked on projects addressing real world challenges in humanitarian and data driven context. One of the fieldlabs was mainly focused on the study, design and development of an emergency incident reporting system for refugees which closed linked with the objectives of this thesis.

At the advice of the thesis supervisor (who was also the course instructor) the author of this thesis collaborated with this fieldlab. The collaboration was set as both fieldlab and the thesis addressed the same overarching problem, how to design an ethically responsible, decentralized system for collecting and sharing sensitive refugee incident data. This created an opportunity for knowledge exchange between individual research condcuted for thesis and collective work carried out within fieldlab.

The fieldlab worked over a period of approximately 3 months and involved weekly in person sessions as well as additional online meetings. during these sessions students and the author jointly discussed conceptual ideas, ethical concerns and technical approaches related to decentralized data architectures, consent based data sharing and humanitarian information system. The collaboration also extended to shared work on code repositories where design ideas were translated to technical implementations. Documentation of this collaboration including the division of tasks and shared development activities is provided separately.

In addition to the fieldlab the research included expert engagement sessions which informed both conceptual and technical dimensions of the study. Together with members of fieldlab the author participated in meetings with an external researcher Dr. Beatriz Esteves (Postdoctoral Researcher, KNoWS, IDLab, Ghent University - imec) who provided guidance on decentralized data infrastructures, use of Solid pods and alternative to centralized triple stores. These discussions lead to decision regarding use of technology like SPARQL (a query language for retrieving data from RDF based databases) and Comunica (a federated query engine which allows querying across multiple distributed data sources) while remaining aligned with ethical priorities of research. Dr. Esteves acted as a resource person giving expert input on decentralized infrastructure considerations.

Further meeting was conducted with Onesmus Wanjiku (Senior FAIR Data Engineer specializing in FAIR Data Point architecture and ETL pipeline for sovereign data systems) who acted as a technical resource person, to discuss deployment related considerations including system feasibility. These interaction served to contextualize research within realistic operational environment.

Though fieldlab collaboration formed an important part of the research the thesis itself stays an individual research project. The author carried out independent empirical data collection in the form of interviews with NGO representatives and refugees which are analyzed separately in this study.

3.4 Data Collection and Analysis

Data collection and analysis were done via multiple methods to guarantee rich understanding of the problem. These methods include like literature review, semi structured interviews with NGO representatives and refugees and participatory engagement via university fieldlab. Each method contributed to different form of data which together inform the research questions and support the iterative development and evaluation of proposed system.

Timeline of Data Collection

Data collection for this study was carried out between September, 20025 and February, 2026 and followed an iterative design oriented approach.

- The literature review was conducted between September, 2025 and February, 2026.
- Interviews with NGO representatives were carried out in December, 2025.
- Interviews with refugee participants were carried out in December, 2025 - January, 2026.
- Fieldlab participation and iterative prototype development took place between October - December, 2025.

Geographical Context of Data Collection

The researcher (author) was based in Netherlands during the study. All interviews were carried

out online via Zoom to allow participation across different geographical locations.

One NGO representative and one refugee participant were based in Kenya. The second NGO representative and four refugee participants were based in Ethiopia.

The following table gives an overview of the types of data collected in this study, their collection methods and the chapters in which they are mainly discussed:

Table 3.1: Overview of Data Sources and Their Analytical Use

Chapter	**Type of Data**	**Collection Method**
Chapter 4 – Literature Review	Academic literature on refugee data systems, decentralized architectures, data sovereignty, humanitarian ethics, FAIR principals and technology adoption	Systematic literature review using structured search strategy, corpus screening, thematic analysis and recommendations from thesis supervisor
Chapter 5 – Needs Analysis: Refugee and NGO Requirements	Empirical interview data (2 NGO representatives, 5 refugees), researcher (author) notes, thematic analysis and convergence divergence analytical sheet	Semi structured interviews conducted via Zoom (1 refugee in english, 4 via Tigrinya translation, NGO interviews in english), audio recorded with consent, structured excel based coding and comparative thematic analysis
Chapter 6 – System Requirements and Design Specifications	Derived functional and non functional requirements	Translation of empirical themes into design principals and technical specifications
Chapter 7 – System Implementation and Deployment	Prototype artefacts	Iterative prototype development in collaboration with the Fiedlab
Chapter 8 – Adoption Potential	Interview derived insights mapped to UTAUT constructs	Thematic analysis of empirical interview data aligned with adoption framework constructs

3.4.1 Literature Review

A systematic literature review formed basis of this research. Academic literature was reviewed across different domains like digital identity systems, humanitarian information systems, refugee data practices, data ethics, decentralized architectures and data governance.

A structured approach was taken to identify, select and analyze the literature reviewed in this chapter. This ensures that materials included are relevant to the aim of the thesis like understanding existing research on refugee data management, humnaitarian information systems, decentralised architectures and technology adoption.

Search Strategy

The literature combined 3 methods:

1. keyword based searches
2. citation chaining using ResearchRabbit

3. targeted inclusion of reports relevant to the study

In addition to database driven search methods the literature selection was informed by key themes and ideas identified during discussions with the supervisor. Several papers were given by the supervisor as initial reference points and certain themes and ideas discussed were used to guide targeted keyword searches using Google Scholar. This allowed spotting of additional studies related to suggested concepts like [12], [13], [21].

Keyword Search
Database searches were performed using Google scholar. A boolean query was developed to capture literature at the intersection of refugee data, digital identity, personal data stores and privacy.

('refugee' OR 'migrant' OR 'asylum seeker') AND ('digital identity' OR 'data protection' OR 'document upload' OR 'personal data store' OR 'data sharing' OR 'privacy')

This query returned a wide range of studies spanning information systems, humanitarian innovation and digital identity.

Citation Chaining
ResearchRabbit was used to explore forward and backward citation networks of key papers. It helps find conceptually related works like in our case in areas like humanitarian data ethics, digital identity systems, decentralised architectures and semantic interoperability.

Targeted Inclusion of Humanitarian Reports
In addition to literature practitioner oriented sources like World Refugee Council (WRC) research paper [1] and case study [2] were included. These documents give applied insights into operational challenges, risks and expectations within real humanitarian settings.

Composition of the Corpus

The final corpus analysed in this chapter includes peer review academic articles, ethical analyses of humanitarian experimentation, papers on solid, linked data, privacy engineering and these sources collectively represent diverse yet interesting perspectives: technical, ethical, operational and theoretical.

Analytical Approach

The chosen literature was analyzed thematically to spot recurring concepts, debates across the reviewed domains. Specific attention was given to themes relating to refugee data agency, consent, fragmentation and structural challenges in humanitarian information systems, semantic modeling and structured data practice, decentralized architecture, personal data store, federated querying and linked data approaches, usability and technological adoption in humanitarian context.
Within the themes literature was examined to extract insights, understand varying perspectives as well as converging viewpoints. This thematic analysis gives a structured basis for further chapters that build on these theoretical insights.

The literature review was important for establishing both theoretical and empirical background of this study. It helped spotting existing challenges related to refugee agency, data protection, trust and interoperability in humanitarian data systems. Moreover it also revealed gaps in existing research relating to the application of decentralized and consent driven technologies in refugee contexts.

3.4.2 Interviews with NGO Representatives and Refugee Participants

Data Collection

An overview of interviewees and focus group participants is provided in appendix A. All of these interviews were conducted online using the application 'Zoom'. Participation was voluntary and informed consent was taken from each participant prior to interview. Participants were informed about purpose of research, intended use of data, confidentiality, anoymisation and their right to withdraw at any time without consequence.

All interviews were audio recorded with explicit consent of participants. Zoom's automatic transcription was enabled during interviews to generate transcripts. In addition the researcher (author) took written notes during each interview to document observations, key reflections and emerging insights.

Two NGO representatives participated in this study and both interviews were conducted in english. Semi structured interviews (Demo demonstration and verbal discussion) were carried out with 2 NGO representatives: Ms. Makeda Saba (Co-Founder of Sanctuary Foundation NGO, Kenya) and Mr. Danial Zemschal Tesfahans (Lecturer and Researcher at Aksum Univeristy, Ethiopia). These participants were chosen because of their professional involvement in humanitarian operations related to refugee support.

The interviews aimed to understand organizational workflows, data needs, ethical constraints and practical challenges faced by NGOs when collecting, analyzing and acting on refugee related information. It was also understood how NGOs access incident data, what types of information are important and actionable and how concerns around privacy, consent and trust influence use of data.

In addition to organisational viewpoints qualitative interviews were carried out with 5 refugees. These interviews were important for grounding research in lived experience and guaranteeing the study did not rely only on institutional viewpoints.

One refugee interview was carried out directly in english. This refugee's contact was provided by the first NGO representative. The remaining four interviews were conducted with the help of second NGO representative who acted as a translator and who also helped arrange these four interviews. During these interviews questions were translated from English into Tigrinya and participant's responses were translated back into English in real time. The analysis of these interviews relied on english translations provided during the sessions and notes to ensure consistency.

Ethical considerations were important for this data collection process. Participation was voluntary, informed consent was obtained and all interviews were carried out with sensitivity to participant's safety, anonymity and well being. No identifying information is share or disclosed in this thesis.

All refugee participants were anonymized at the point of transcription and analysis. Identifying details like names, specifications locations, organizational affiliations or personal identifiers were neither recorded nor used anywhere in the thesis. Participants are referred to in this thesis using non identifiable labels (Ref-A, R1, R2, R3, R4). Only anonymized excerpts are user for analysis.

Given the vulnerability of refugee participants care was taken in interview process. Participants were approached via trusted contacts (provided by the first supervisor) to avoid coercion and ensure participation was perceived as voluntary and independent from any instituional service provision. At the beginnning of each interview the researcher assured the participants that their information would be kept safe, anonymized and not disclosed to anyone beyond this academic scope. Also the video feature was turned off and not recorded to ensure further safety. Interviews were conducted in a way whuch prioritized psychological safety allwoing partiicpants to decline questions or pause discussion at any time.

The interviews focused on refugee's experiences with reporting incidents, interacting humanitarian organizations and sharing personal information. Topics included perceived risk of data sharing, trust in institutions and expectations regarding privacy and control over personal data.

The links to full interview transcript files are listed in appendix B while participant details are given in the table A.1.

Data Analysis

Interview data collected from NGO representatives and refugees were analyzed using a thematic analysis approach. After each interview notes were reviewed to familarize with the content. Analysis proceeded in multiple states to guarantee systematic interpretation. The transcripts were reviewed to get data familiarization. Codes were assigned to segments of data which reflected recurring ideas, concerns or experiences like issues of trust, data sharing risks, perceived usefulness of reporting mechanisms and expectations regarding control over personal information.

These codes were then grouped into broader themes which captured shared patterns across participants while still allowing for differences between stakeholder groups. Themes were organized separately for NGO and refugee participants. For example themes related to organizational data needs and operational constraints emerged mainly from NGO interviews whereas themes relating to fear of surveillance, consent and personal safety were more noticeable in refugee's interviews.

To systematically examine alignment and tensions between participants a structured convergence divergence anlaysis sheet was developed (appendix C). This sheet helped identify:

- Areas of convergence

- Areas of divergence

In a further layer selected themes were mapped onto constructs of the Unified Theory of Acceptance and Use of Technology (UTAUT) [12]. Interview excerpts were examined in relation to performance expectancy, effort expectancy, social influence, facilitating conditions and behavioural intention. This mapping supported later evaluation of adoption potential. The links to coding labelling document as well as convergence divergence analysis document are listed in appendix C.

The purpose of this analysis was not for quantifying responses but for identifying important themes which could inform system requirements addresses in later chapters. The themes obtained from interview data directly helped interpretation of stakeholder needs (RQ1) and considerations relating to adoption and trust (RQ4).

3.4.3 FieldLab Participation and Prototype Development

In addition to interviews and literature review the research involved iterative development of a functional prototype of the proposed emergency incident reporting system. The prototype was built in collaboration with Fieldlab. An overview of the collaborative development is given in appendix E.

The development process followed iterative and collaborative cycle. Features were built incrementally, reviewed, refined over multiple rounds of interaction. This continuous exchange guaranteed alignment between theoretical concepts and technical implementation.

The prototype development process was documented using a controlled GitHub repository (appendix D). All implementation iterations and feature refinements were recorded via structured commits and commit messages allowing traceability of design evolution over time. Code, files etc were maintained in a proper structure to ensure clarity and reproducibility. GitHub's history provides an auditable record of incremental changes aligned with feedback from fieldlab discussions. This documentation approach supports transparency, iterative refinement in the technical development process.

Data Analysis

Prototype artefacts were examined as evolving objects embedded within iterative decision making process.

Fieldlab discussions, meeitng notes and feedback sessions were reviewed to spot recurring technical and governance considerations. Particular attention was given to decentralization principals, practical feasibility and sakeholder expectations.

Prototype artefacts like access control configurations, interface mock ups and github commits were treated as analytical material.

The major implementation decision like private by default storage, consent based access control etc was examined against ethical principals spotted in literature review, operational feasibility discussed in fieldlab sessions etc.

This artefact based analysis allowed translation of concepts like selective sharing into concrete technical features. The iterative refinement process also showed constraints, trade offs and challenges which were documented as part of research findings.

3.5 Mapping Methods to Research Questions

RQ1: Needs - What are the needs and priorities of both refugees and NGOs in relation to data recording, sharing and analysis?

RQ1 was mainly addressed using semi structured interviews with refugees and NGO representatives. Interviews with refugees focused on lived experiences relating to safety, barriers, trust and control over personal data. Interviews with NGO representatives explored organizational needs, priorities and constraints relating too incident reporting, data analysis.

These empirical insights were complemented with literature review which talks about broader discussions on humanitarian data practices, power imbalances and ethical risks associated with refugee data collection.

RQ2: Specifications and Requirements - What are the functional and non functional spec- ifications required for designing a solid based emergency reporting system that meets these needs while safeguarding privacy, consent and digital agency?

RQ2 was addressed by translating needs and priorities in RQ1 into functional and non functional system requirements. This translation was supported by literature review which gave concepts and design principals relating to decentralized data architectures, privacy by design, consent based access control and digital agency.

Participation in fieldlab also contributed to refine these requirements via iterative design discussions and collaborative reflection. Identified needs like user control over data, selective sharing, interoperability and ethical safeguards were mapped to specific functional requirements (eg access control mechanism, data structuring) and non functional requirements (eg privacy, security).

RQ3: Deployment - How can such a system be implemented and deployed in a technically feasible manner that meets the identified specifications?

RQ3 was addressed mainly via fieldlab participation and expert discussions relating to system implementation and deployment. Collaborative design sessions and technical work helped explore feasibility issues like decentralized querying, deployment etc.

Additional expert (**'Onesmus'**) input gave practical viewpoints on deployment considerations allowing the research to assess how proposed system could function in realistic environment.

RQ4: Adoption potential - What is the potential for adoption of this system by refugees and NGOs considering usability, trust and ethical acceptability?

RQ4 was addressed via interviews with refugees and NGO representatives. Refugee interviews were specially important for understanding trust related concerns including fear of surveillance, misuse of data etc. NGO interviews contributed viewpoints of usability and ethical responsibility.

3.6 Ethical Considerations

This research deals with very sensitive context including refugees, humanitarian organizations and handling of personal information. Ethical considerations thus played an important role throughout the research affecting decisions relating to data collection, participant engagement, analysis and overall research design.

3.6.1 Informed Consent

Informed consent was a fundamental requirement for all data collection tasks. All interview participants were told about the purpose of research, nature of participation and how the information they gave would be used within the scope of thesis. Participation was voluntary and participants were made aware that they could decline to answer specific questions or withdraw at any time without consequence.

In case of refugee interviews special care was taken to ensure consent was meaningful and not just assumed. The study avoided technical language and focused on clear explanation to support understanding of participant. This was to respect participant's autonomy and reduce risk of coerced participation.

3.6.2 Anonymity and Confidentiality

Because of the sensitivity of subject matter anonymity and confidentiality were prioritised throughout the study. Names of refugee participants were not recorded or noted.

All gathered data was handled with care and used only for academic purposes within scope of this research. There measures were taken to minimize possible risks to participants particularly refugees for whom disclosure of personal information could have serious consequence.

3.6.3 Power Imbalances and Refugee Vulnerability

Refugees frequently occupy vulnerable positions and may feel pressure to participate in research linked with institutions or aid related context. This study tried to remove those imbalances by adopting respectful, non intrusive approach and by framing participants as contributors of expertise based on lived experience instead of subjects if study.

Questions were made to focus on experiences, needs and viewpoints instead of traumatic

events and participants were not asked to give away details they were uncomfortable sharing. This aligns with practices which stress harm minimization and participant well being.

3.6.4 Ethics by Design

The emphasis on decentralization, consent based sharing and user control reflects an ethical stance which prioritize refugee agency and data protection. Instead of treating ethics as an external factor this study integrates ethical principals directly into both methodological choices and system design considerations.

3.7 Synthesis

This chapter outlined the research approach, study design and methodological choices. this study was set as a design oriented and participatory research project situated within a real world academic and humanitarian context. Instead of separating technical development from empirical inquiry the research combined qualitative methods with collaborative design activities to explore how a refugee centered emergency incident reporting system could be conceived, implemented and assessed.

Multiple data collection methods were used to address research question. Literature review gave theoretical and contextual basis for understanding humanitarian data practices, decentralized systems and ethical challenges. Interviews with NGO representatives, refugees and experts gave insight into practical need, priorities and constraints while participation in fieldlab allowed iterative reflection on design decisions, technical feasibility and ethical trade offs.

The data analysis approach focused on synthesizing insights across those sources instead of treating them in isolation. Interview findings were analyzed thematically and understood alongside insights from literature and fieldlab discussion. This synthesis helped translation of identified needs into functional and non functional requirements directly affecting the design and deployment decisions.

Ethical considerations were important to both research process and design orientation of study. Issues of consent, anonymity, power imbalance and refugee vulnerability were addressed throughout research. By putting ethical reflection into methodological choices the study tried to ensure that both research process and resulting system aligned with humanitarian principals.

Overall this chapter sets the methodological foundation for the remainder of thesis. The chapters 5-8 build on this foundation by presenting findings, system design and evaluation outcomes obtained from methods described here.

Chapter 4

Overview of the Literature Review

4.1 Introduction

The goal of this chapter is to give an in depth review of the academic literature related to digital data practices, technological interventions and challenges in humanitarian contexts. The aim is to explore existing research systematically to identify technical and ethical debates that emerge from humanitarian debates and that have shaped the use of digital systems when working with vulnerable populations like refugees.

This chapter gives an understanding of existing scholarship on refugee data management, user agency and responsible use of information technologies. The review is organised to examine literature on refugee data practices and user agency, work on semantic modeling, ontologies and humanitarian common data standards, research on decentralised web architectures and Solid pods, studies on usability and technological adoption in humanitarian context.

4.2 Refugee Data Systems and User Agency

Research on refugee data practices continuously highlight the structural, ethical challenges that pop up when humanitarian actors collect and manage personal information from displaced populations. Instead of treating refugees as passive data subjects recent studies examine how digital systems shape autonomy and capacity of displaced individuals to represent their situations. This literature gives vital insights into how digital systems could shape autonomy, representation and control for displaced individuals stressing recurring problems across humanitarian research.

4.2.1 Data Agency and Power Asymmetries in Humanitarian Contexts

A core concern in modern refugee studies is the continuous imbalance of power between refugees and institutions that collect their data. A previous study [1] argues that digital identity infrastructures often reproduce existing problems by concentrating control in the hands of humanitarian organisations, states or technology providers. Refugees have little understanding of how their personal information is used. This lack of agency is not just an ethical issue but a technical design problem because systems which do not involve mechanisms for user control,

transparency and revocability risk reinforce dependency and mistrust.
The idea of 'data agency' thus emerges as a central theme in this literature stressing how control over personal data, transaparency of data use and meaningful consent mechanisms are critical for addressing power imbalance in humanitarian information systems [3].

4.2.2 Fragmentation, Inconsistency and Information Loss in Refugee Data Practices

Multiple studies show how humanitarian information systems struggle with fragmentation and inconsistency. A study [2] in their analysis of digital identity systems for refugees describe environments where data is captured in incompatible formats, stored in isolated databases. These practices result in duplicated record, loss of critical information and an inability to coordinate effectively across organisations. The literature positions structured data models as essential tools for addressing these challenges.

4.2.3 Ethical Risks in Humanitarian Data Collection

The literature [5] present a taxonomy of risks linked with humanitarian experimentation emphasising that new technologies can unintentionally expose refugees to harm. Key concerns could be insufficient informed consent and unclear data flow.
Some researchers [4] in their study of 'data hubris' argue that humanitarian organisations often overestimate their ability to process and interpret complex datasets while underestimating the potential for harm. These insights point to the structural requirements of any humanitarian data system which are clear communication of purpose, minimal data collection, traceability of data access and user control over sharing. The literature continuously stresses importance of clear communication of data practices, informed consent, minimal data collection and user control about data sharing as important safeguards in humanitarian data systems [4, 5].

4.2.4 Trust, Autonmoy and Sociotechnical Alignment

Researchers stress on the importance of trust in digital systems involving refugees. Trust is affected not just by organisational behaviour but also by the technical architecture. Prior research [3] show that misalignments between digital identity systems and refugees' lived social realities along with limited opportunities for refugees to influence how they are identified can create tensions and vulnerabilities that undermine the protective aims of these systems. While systems that offer transparency and user choice are more likely to be seen as legitimate and respectful. Previous studies suggest user controlled data architecture and decentralized models may help build trust by aligning technical system behaviour with refugee's lived realities and expectations specifically in context characterized by vulnerability and power imbalance [3].

4.3 Semantic Modelling, Structured Reporting and Common Data Models

The literature on humanitarian systems highlights a gap between the volume of data collected and the ability to interpret if in meaningful, accountable way. [4] show how enthusiasm for data revolution and crisis mapping often outsrips the analytical and organisational capacity needed

to use these datasets responsibly. In such settings incident reports are frequently captured in ad hoc formats tied to specific platforms and difficult to aggregate across organisations. This underlines the need for better structured data models that make incidents comparable, traceable and interpretable over time.

The research [9] describe the solid protocol as a layer for distributed knowledge graphs in which personal data is stored in RDF based resources within user controlled pods and accessed by applications. Solid' reliance on semantic web standards means that the data is modelled as triples. This architecture is designed to enhance data sovereignty and interoperabiltiy, the same RDF resources can be reused by multiple applications without being copied into new centralised databases.

Recent work suggest how this semantic approach can support privacy preserving applications handling sensitive personal information. A previous study [8] present SocialGenPod a system in which user data is stored in solid pods and accessed via controlled retrieval mechanisms. Although SocialGenPod targets personal AI assistants rather than humanitarian reporting it suggests that semantically modeled data in pods can aid complex, cross application workflows without sacrificing user control.

Within refugee and migration studies [2, 3] authors highlight how existing digital identity infrastructures tend to be fragmented, centralised with refugees' records distributed over multiple databases that are not interoperable and often inaccessible to the individuals themselves.

4.4 Decentralised Architectures and Solid Pods

A growing body of research in web architecture, privacy engineering and personal data management talks about the dominance of centralised data platforms and explores alternatives that distribute control back to end users. Within this landscape decentralised architectures particularly those based on solid protocol have emerged as promising approaches for addressing long standing concerns regarding data sovereignty, access transparency and interoperability.

An existing paper [9] give a detailed examination of solid from a privacy and security perspective. Their analysis describes solid pods as user controlled storage spaces containing personal data represented in RDF. Unlike traditional platforms in which personal information is stored and processed within controlled servers, solid enables individuals to determine where their data resides and which applications may access it. This model enhances compliance with data protection obligations by separating identity, storage and application layers thereby reducing the power imbalances in centralised systems.

Work on decentralised personal data stores also highlight the role of semantic web standards in enabling flexible, cross application reusage of data. In the socialgenpod study [8] it is discussed how solid pods can support privacy preserving applications by keeping user data in decentralised, user controlled stores rather than centralised platforms. This reinforces a principal in decentralised systems that when data is stored as linked, machine readable resources under the user's control applications can interoperate without relying on institutions.

The ethical literature further strengthens the argument for exploring decentralised models. Studies [4] warn that humanitarian organisations often collect vast amount of sensitive data without having the analytical capacity to interpret it responsibly. They argue that this overconfidence can increase the consequences of misuse. Decentralised architectures by distributing data ownership and minimising unnecessary aggregation align with need for reducing institutional accumulation of sensitive information.

Across these studies various themes emerge. First decentralised architecture provide a structural mechanism for strenghtening user agency by separating data storage from application logic. Next solid and related systems leverage semantic web standards to support interoperability without centralisation. Additionally existing studies identifies risk in current centralised data infrastructures that decentralised models are uniquely positioned to address. Lastly decentralisation aligns with ethical concerns about power, transparency in humanitarian data practices.

Together these insights form a foundation for understanding why decentralised, user controlled data models are increasingly explored in domains where personal information is highly sensitive, including refugee protection and humanitarian response.

4.5 Federated Querying and Linked Data Analytics

Humanitarian information systems face continuous challenges of fragmentation, inconsistent data formats and limited interoperability across organisations. Existing studies [2] describe refugee data ecosystems as characterised by 'silos' of information that prevent coordinated action and prevent organisations from forming a coherent understanding of risks or needs across cases.

Linked data technologies and RDF based representations provide such pathway. Because RDF encodes information as machine readable triples with semantic relationships it supports the possibility of running queries across distributed sources without requiring data consolidation. Interoperability is not achieved by merging datasets into a central repository but by aligning their meaning through shared vocab and schemas.

Federated quering extends this logic by enabling queries to run across multiple decentralised datasets simultaneously. Rather than extracting data from refugees' personal stores into organisation servers federated engines send the query to each data source and assemble the results dynamically. This approach goes in opposite to the centralised big data systems. Prior studies [4] describe how organisations often overestimate their capabilities, collecting large volumes of information that they struggle to interpret. Federated querying mitigates this risk by allowing organisations to work only with the specific data they are authorised to access at the moment of analysis reducing unneccessary accumulation of sensitive informatinon and supporting a more targeted, capacity aligned process.

Ethically federated querying aligns with concerns raised in the literature [5] where scholars argue that experimental humanitarian systems which collect and process match large volumes of sensitive information may unintentionally expose individuals to harm when deployed with-

out safeguards. By distributing storage and enforcing consent based access federated analytics avoid creating large, high risk repositories.

Federated analytics bypass the need for institutional consolidation by enabling organisations to extract meaningful insights from structured personal data without requiring a shared database or central authority. As long as data is semantically aligned via linked data standards like RDF and shared ontologies like the Common Data Model federated querying becomes a practical strategy for cross organisational interoperability.

4.6 Usability and Technology Adoption

Digital systems intended for refugee must be evaluated not only on their technical robustness but also on their usability, accessibility and likelihood of adoption. Technology adoption is shaped by factors far beyond functionality like trust, clearity of purpose, ease of use and alignment with the lived experiences of its intended users.

A central thing is adoption of trust which has repeatedly been highlighted as delicate in refugee ecosystems. Studies [2] note that refugees often lack clear understanding of how their data is used which leads to hesitation. Similarly related research [5] show that past experiences with surveillance or opaque data practices reduce confidence in digital platforms and directly affect adoption.

Existing studies [3] emphasise refugee facing systems often fail when their design reflects organisational priorities rather than refugee realities. For people digital literacy levels vary substantially and any system that demands high technical skill risks excluding those most vulnerable. Research [10] shows how meaningful participation requires tools that are intuitive and responsive to users' communicative norms.

Multilingual design comes out as a crucial dimension of usability in humanitarian systems. Refugees often speak languages which are are not commonly used in digital infrastructures. Prior research [1] stresses that ethical digital systems must ensure that refugee understand what data they are providing and why noting that language gaps can easily lead to uninformed participation.

Studies [4] caution that systems designed around data collection rather than needs of user often fail to deliver value to communities they intended to serve. These things align with classical adoption theories [12, 24] like perceived usefulness, perceived ease of use and compatibility which hold that users adopt technologies only when the benefits outweigh the effort and risk.

Altogether the literature tells that system adoption in refugee contexts is a trust dependent, context dependent and language dependent process. A system must be easy to navigate, available in languages user understand and aligned with principals that prioritize dignity, agency and safety. Multilingual support. transparency in data flows and explicit user control are thus key determinants of whether a technological intervention will be accepted and used menaingfully by refugees and NGOs.

4.7 Synthesis

Across the things reviewed in this chapter the literature converges on various principals which shape the thinking on humanitarian data systems.

Firstly research on refugee data practices highlights the persistent power imbalances, lack of agency and widespread mistrust in existing humanitarian information systems. Refugees often have less control over their and limited visibilty into how it is used.

Secondly studies on semantic modeling and humanitarian data standards stress the importance of structured, interoperable representations of incident information. RDF based modeling and shared vocabularies help address fragmentation and enable menaingful comnparison across reports without requiring data centralisation.

Thirdly decentralised structures and linked data literature point to solid pods as an ethically aligned alternative to centralised databases. By keeping the data under usr control and enabling permissions decentralisation responds to concerns about data hubris, experimental systems and the risks of large scale aggregation.

Fourth, federated querying comes out as a practical mechanism for enabling NGO to detect patterns across distributed refugee records. It allows analytical insight without creating new central repositories thus balancing operational needs with ethical constraints.

Lastly the literature on usability and technological adoption stresses that systems must be accessible, trusted and contextually aligned. Refugees are more likely to adopt technologies that are understandable and visibly protective of their rights.

Chapter 5

Needs Analysis: Refugee and NGO Requirements

5.1 Introduction

This chapter talks about the first sub research question (RQ1):What are the needs and priorities of both refugees and NGOs in relation to emergency data recording, sharing and analysis?

The motive of this chapter is to identify these needs based on empirical evidence and existing literature so as to give a grounded foundation for further system requirements. Understanding these stakeholder needs is an important requirement for the design of any system which is supposed to operate within humanitarian context. Without a clear understanding of stakeholder priorities technological creations risk again creating existing power imbalances introducing different forms of harm or failing to gain trust.

The need analysis show in this chapter is grounded in 2 complementary sources. first it draws on insights gathered from interviews conducted with representatives from humanitarian organisations and refugee participants. Refugee interviews explored experience and tensions relating to documenting of emergency situations, controlling personal data, interacting with digital systems and accessing organizational support. Interviews with NGO representatives helped think about organizational requirements, ethical considerations and challenges relating to emergency data management and analysis. second the chapters integrates insights from existing literature on refugee's data management and humanitarian information system which talk about repeated issues like fragmented data infrastructures, limited transparency coercive data collection and restricted agency for displaced people.

To preserve anonymity while maintaining traceability interview participants particularly refugees are referenced using anonymized codes throughout this chapter. Refugee participants are identified as Ref-A, R1, R2, R3 and R4 while NGO representatives are referenced using NGO-A and NGO-B, as documented in the table A.1 listed under appendix A.

The focus of this chapter is on articulating needs rather than evaluating technologic solutions. Interview outcomes are understood as expressions of underlying requirements, concerns and constraints that shape the way emergency data systems should be conceived in refugee contexts. This approach lets the analysis stay grounded in stakeholder perspectives. By focus-

ing on needs at this level the chapter sets a conceptual foundation which can inform subsequent discussions of system requirements and design choices.

The chapter is structured as follow: section 5.2 outline the empirical data sources and analytical approach used to derive needs and priorities from interview material including qualitative coding process and convergence divergence analysis across stakeholders, section 5.3 explores refugee needs and priorities relating to emergency data recording involving issues of privacy, consent trust, acessibility and the diversity of refugee experiences, section 5.4 explores the needs and priorities of NGOs focusing on requirements for structured information, interoperability, ethical access to sensitive data and analytical capabilities for finding patterns across cases, section 5.5 synthesizes these perspectives to assemble system level priorities which emerge from the combined needs of both groups stressing the need to balance refugee protection with organisational effectiveness, section 5.6 summarizes the key findings and prepares the transition into the following chapter where these needs are translated into concrete system requirements and design specifications.

5.2 Data Sources and Analytical Approach

The empirical material which helps in the needs assessment contains 5 interviews conducted with refugee participants and 2 interviews conducted with NGO participants. An overview of all interviews including participant identifiers, language and mode of interaction is provided in appendix A. Full interview transcripts are available in an external repository as detailed in appendix B.

5.2.1 Coding and Thematic Analysis

The interview data was analyzed using a qualitative coding approach. Interview notes were reviewed to spot recurring concerns, expectations, risks and constraints expressed by participants in relation to emergency data practices. Instead of applying predefined coding scheme codes were developed directly from interview material to guarantee that analysis remain grounded in the viewpoint of participants.

Initial open coding was done across all interviews to label text reflecting issues or needs like concerns about privacy, control over personal information, accessibility or organizational data use. Related codes were grouped into high level thematic categories representing shared or contrasting needs.

The coding and labelling process was documented in a structured spreadsheet. The analytical artefact is provided in appendix C.

5.2.2 Convergence and Divergence Analysis

A convergence divergence analysis was carried out following the thematic coding. This step focused on areas where perspectives aligned within as well as across stakeholder groups.

Themes emerging from interviews were analyzed to assess whether they reflected shared objectives or conflicting ones. This comparison allowed spotting of system level implications arising

from both convergence and divergence.

The outcomes of this comparative analysis was documented in a convergence divergence spreadsheet which summarize point of alignment as well as difference between participant's viewpoints. This document is given in appendix C.

5.3 Refugee Needs and Priorities in Emergency Data Recording

Refugees who experience violence, exploitation, detention or other emergency situations face various barriers to document their experiences in ways that are safe as well as meaningful. Existing practices often ask displaced people to continuously give away sensitive information under conditions of stress, uncertainity and unequal power relations.

5.3.1 Privacy, Data Minimisation and Protection from Harm

A main priority for refugees is protection of sensitive personal information and prevention of unintended data exposure while documenting emergency situations. Participants continuously framed safety in terms of who can access their information and under what conditions instead of viewing privacy as a secondary concern. Emergency data often involves details relating to identity, location, experiences of violence, health conditions or family relationships. If not handled properly this information can expose refugees to serious risks like surveillance, exclusion from services or retraumatisation. Interview insights stressed that current practices frequently ask refugee to disclose more information than what is necessary sometimes again and again and across organisations increasing the possibility of harm.

When asked about visibility of emergency related data refugee participants indicated personal information should remain private by default and accessible only to individual when explicit permission is given. Responses showed unrestricted or automatic access by external people would reduce participant's willingness to document sensitive situations. This concern was expressed across interviews with refugee participants (Ref-A, R1, R3 listed in appendix A).

Participants (R3, R4 as under table A.1)also indicated ability to limit amount and sensitivity of information shared like location data, images, contact details was important specially in situations involving stress, fear or time pressure. Optional data fields were seen as allowing refugees to document emergencies without being forced to disclose information they saw as risky. This stresses a strong need for data minimisation in emergency reporting cases. Refugees prioritise systems which limit data collection to necessary information and avoid unnecessary personal identifiers. Minimising exposure is not just a concern of privacy but also a protective strategy in environments where refugees may be subject to coercion or where access to personal devices could be forcibly obtained. The literature similarly talks about how excessive data collection in humanitarian contexts can undermine protection goals and increase vulnerability rather than prevent it.

Privacy in this context is thus not just about confidentially but also about reducing the possible consequences of data misuse. Refugees need mechanisms which avoid sensitive information

from being easily accessible, shareable or transferable without clear justification. Systems which fail to prioritise minimisation risk reinforcing power imbalances by treating refugees as passive data sources instead of individuals whose safety depends on careful handling of information. The underlying interview evidence supporting analysis is given in annexed interview transcripts (see appendix B).

5.3.2 Data Ownership, Consent and Control

In addition to tensions about privacy and minimization the refugee interviews stressed a strong need for clarity around data ownership and meaningful control over consent. Participants indicated emergency related information should be understood as belonging to individual who creates it instead of the system or external organization by default.

When discussing about ownership of information participants (Ref-A, R1, R2, R3, R4 (A.1)) expressed they expected to remain primary decision makers regarding how their data is stored, accessed and reused. Responses across interviews suggested uncertainity about data ownership could undermine trust in digital systems specially in humanitarian context where refugee may already feel disempowered.

Closely related to ownership was need for explicit and informed consent. Participants (R4 (A.1)) indicated consent should not be assumed or implicit but instead given explicitly for specific recipients. Interview responses suggest that refugee would be more willing to document sensitive situations if they could clearly understand what they were consenting to. This include clarity regarding which organization could access data.

Also participant stressed that consent should be reversible. They indicated that trust in organization may change due to personal experiences or changing circumstances and system should thus allow users to withdraw previous granted consent. The ability to revoke access was described as important for maintaining safety and agency over time.

Addressing these needs is important for guaranteeing emergency data system support refugee autonomy instead of reproducing existing power imbalance. The interview evidence underlying this analysis is documented in annexed transcripts and coding artefacts (see appendices B and C).

5.3.3 Trust, Psychological Safety and Fear of Technical Interfaces

Beyond privacy and consent refugee interviews showed that trust in digital systems is closely linked to feelings of psychological safety and perceptions of technological ris. Participants (Ref-A, R2, R4 (A.1)) indicated willingness to engage with an emergency data system depend not only on formal safeguards but also on whether the system feels understandable, predictable non threatening in moments of stress.

When asked about interacting with digital tools during emergency situations participants suggested that complexity, lack of transparency could increase anxiety instead of reducing it.

Trust was described as something which develops slowly. Participants (Ref-A (A.1)) indicated trust increases when system functions are easy to understand when users feel confident that they are not being monitored without their knowledge. Ambiguity about system logic was seen as a source of discomfort especially in stressful context.

Psychological safety was also linked to perceived vulnerability. Participants noted emergency situations often involve fear, urgency making it difficult to engage with systems which require multiple decisions. In such context even small uncertainity could discourage use.

Guaranteeing psychological safety via clarity, transparency and low technological risk is therefore a key priority for refugees. The interview evidence informing the analysis is given in annexed transcripts (see appendix B).

5.3.4 Language Accessibility and Inclusivity

Refugee interviews highlighted language accessibility as a fundamental need for informed participation in emergency data recording. Refugees often speak languages which are not represented in digital systems and reliance on dominant languages could create obstacles to understanding, consent and accurate reporting. Participants (Ref-A, R1, R2, R3, R4 (A.1)) indicated that the availability of interfaces in refugee's primary languages highly affects comfort, understanding and willingness to engage.

Beyond basic translation language accessibility relate to guaranteeing that key concepts, warnings and choices are communicated in culturally and linguistically appropriate ways. Participants indicated that limited proficiency in dominant or official language can create significant barrier to safe and accurate documentation specially in stressful situation.

Several participants stressed that language barriers could lead to misunderstandings, incomplete disclosure or uninformed consent. They also hinted that being able to engage with the system in a familiar language increases confidence and reduces anxiety. Refugees therefore prioritise systems which support multilingual interaction as a prerequisite for ethical data collection rather than optional enhancement.

Addressing language accessibility is thus important for guaranteeing that emergency documentation systems are trustworthy. the interview evidence underlying the analysis is documented in annexed transcripts (see appendix B).

5.3.5 Diversity of Refugee Profiles and Situational Constraints

Refugee's needs vary widely depending on factors like age, gender, legal status, previous experiences and immediate situations. Interview insights stressed that some individuals may be more willing or able to document incidents while others may be constrained by fear, urgency trauma or limited access to technology.

This diversity creates a need for flexibility in emergency data recording. Refugees prioritise the ability to choose which information to provide and when rather than being subjected to rigid reporting structures. Situation constraints like time pressure, stress or unsafe environ-

ments also reinforce the importance of adaptable and non intrusive data collection methods.

Recognising diveristy also means acknowledging that refugee's priorities may change over time. What feels safe to disclose at one moment may not feel safe later. Emergency data systems thus must accomodate partial or incremental reporting without penalising users. Addressing this diversity is important for ensuring that emergency documentation supports protection instead of imposing additional burdens on already vulnerable individuals.

5.3.6 Digital Access, Device Availability and Connectivity

Beyond privacy, consent and trust interviews also talked about access to digital infrastructure. Engagement with digital reporting tools supposes access to mobile device, internet connectivity and basic level of digital familiarity. Almost all refugees reported owning or having access to mobile phones. They indicated prior experience with digital applications like banking applications.

In displacement context access to smartphones, stable internet or private device use may not always be guaranteed. Connectivity could be intermittent and dependent on mobile device availability while device access may be shared. These conditions impact how feasible and safe digital engagement may feel in emergency situations.

Digital access should thus be understood as part of broader structural environment within which refugee data practice happen. Availability of devices, connectivity and technological familiarity shape not just practical participation but also perception of risk, autonomy and control.

5.4 NGO Needs and Priorities in Humanitarian Data Use

Humanitarian organisations play an important role in responding to emergencies affecting refugees yet their ability to act effectively is heavily shaped by their duality, structure and accesibility of information available to them. NGOs operate under conditions of limited resources, time pressure and ethical responsibility often relying on fragmented data collected across multiple actors and systems. The needs and priorities talked about in this section reflects insights from interviews with NGO representatives as well as challenges documented in the humanitarian information system literature. Together they highlight that NGOs require data practices which support analysis and coordination while remaining ethically aligned with the protection of vulnerable populations.

5.4.1 Need for Structured and Standardised Incident Data

A primary need identified by NGO representatives is access to structured and standardised incident data. Both NGO representatives (NGO-A (Makeda) and NGO-B (Danial) (A.1)) stressed that existing reporting practices often rely on unstructured narratives, handwritten notes or platform specific forms which make it difficult to compare incidents across individuals, location or time periods. This lack of standardization limits NGO's ability to identify trends, prioritise

interventions or allocate resources effectively.

Structured data allows NGO to move beyond isolated case handling toward more systematic analysis. NGO representatives indicated that when incident attributes like location, type of risk, time frame or expressed needs are recorded consistently organisations can much easily group similar cases and identitfy repeating patterns. Interview insights stressed that structured inputs reduce ambiguity and interpretation effort particularly in high pressure environments where rapid assessment is requirement.

The studies also stress that fragmentation and inconsistency in humanitarian data practices contribute to duplication, of effort and information loss. NGOs thus prioritize reporting mechanisms which impose a minimal but clear structure on data entry ensuring that information remains comparable across cases without requiring extensive manual processing.

The NGO interviews further indicate that structured inputs reduce ambiguity and interpretation effort. The interview evidence supporting this analysis is documented in annexed transcripts (see appendix B).

5.4.2 Interoperability Across Organisations and Systems

Humanitarian response involves multiple organisations operating simultaneously across different regions. As per the interview insights (NGO -A and NGO-B (A.1)) NGOs thus face a continuous challenge of interoperability as data is often stored in incompatible formats.

Interview insights also indicate that interoperability is not just a technical concern but also an organisational one. NGOs require data representations which can be understood and reused across institutional context without extensive transformation. This need is mainly important in cross border operations or in situations where refugees interact with multiple organisations over time.

The studies on humanitarian information systems reinforces that the absence of shared standards affects coordination and reduces the collective effectiveness of response efforts. NGOs thus prioritise approaches which support semantic consistency and shared understanding, allowing data to retain meaning when accessed by different actors. Interoperability is viewed a prerequisite for collaboration instead of an optional enhancement. The interview material underlying this analysis is given in the appendix B.

5.4.3 Ethical Access to Sensitive Refugee Data

While NGOs rewire access to refugee data in order to provide assistance and protection this access must be ethically justified and carefully managed. Interview insights reflected an awareness among NGO representatives of the risks associated with handling highly sensitive information including potential misuse, unauthorised sharing or unintended exposure. This is a strong recognition which data access carries responsibility particularly when dealing with populations at heightened risk.

NGOs thus prioritize data access models which are transparent, accountable and aligned

with humanitarian principals. Ethical access implies organisations should only view information which is relevant to their mandate. This contrasts with practices in which data is broadly collected and stored centrally 'just in case' a pattern which has been criticised as contributing to data accumulation without corresponding safeguards.

The need for ethical access also affects reputation and legal considerations. NGOs operate under increasing survey regarding data protection and accountability. Systems which provide clear boundaries around access help organisations show compliance with ethical standards.

5.4.4 Pattern Detection and Analytical Needs

Beyond individual case management NGOs (NGO-A and NGO-B (A.1) emphasize importance of identifying patterns across incidents. Many risks faced by refugees like repeated detentions, ransome demands or dangerous transit routes only become visible when data from multiple individuals is analysed collectively. Without mechanism for grouping and filtering reports such patterns remain hidden limiting proactive intervention.

Analytical capabilities are thus a key priority. NGOs require the ability to filter incident data by attributes like location, time range, type of risk or expressed needs in order to detect trends. These abilities support evidence based decision making allowing organisations to allocate resources more effectively and make for targeted responses.

At the same time the studies cautions against large scale data aggregation which exceeds organisational capacity. NGOs thus face a tension between the desire for analytical insight and the need to avoid creating high risk data repositories. This tension stresses the importance of analytical approaches which enable pattern detection while respecting constraints related to privacy, consent and proportionality. The interview material informing this analysis is given in appendix B.

5.5 System Level Priorities Emerging from Combined Needs

The system priorities presented in this section are obtained from the thematic coding and convergence divergence analysis described in section 5.2 drawing on both refugee (section 5.3) and NGO (section 5.4)interview data (see appendices B and C). The needs and priorities identified among refugees and NGOs show both shared objectives and tensions. Refugees prioritise safety, control and dignity in the handling of personal information while NGOs require structured, reliable data to support coordination and analysis. These priorities are not incompatible but they place different demands on emergency data systems.

Rather than treating refugee protection and organisational effectiveness as competing goals the analysis highlights that humanitarian data practices must address both together. Systems which prioritise analytical capacity without safeguarding agency risk reinforcing power imbalances while systems which focus exclusively on protection without enabling analysis may limit the ability of NGOs to respond effectively. The requirements identified here thus show the need to balance these concerns in an ethically grounded manner.

5.5.1 Balancing Refugee Agency with Organisational Effectiveness

A main requirement emerging from the combined needs is the ability to balance refugee agency with NGO effectiveness. Refugees need control over what information is recorded and shared while NGOs depend on access to comparable data to spot trends and respond to emergencies. If either side's needs dominate the system risks failure. Excessive control without analytical utility limits organisational action while unrestricted access affects trust and safety.

This balance requires acknowledging that agency is not a hurdle to effectiveness but a condition for it. When refugees perceive data practices as respectful and protective they are more likely to engage in documentation increasing the availability and reliability of information. When data is collected without meaningful control reluctance and partial disclosure reduce data quality and affect analytical value. A system level requirement thus emerges for mechanism which preserve individual agency while still enabling organisations to work with meaningful datasets.

5.5.2 Requirements for Selective Sharing and Access

Both refugee and NGO perspective point towards the need for selective sharing rather than unrestricted access. Refugees stress the importance of deciding which organisations may access their information while NGOs recognize that ethical access requires proportionality and clear justification. Selective sharing in this context refers to controlled organisational access where refugees decide which actors are trusted to view their data and retain the ability to revoke that access as situations change.

This form of selective sharing addresses the concerns related to coercion, misuse and over collection by avoiding default or universal visibilty of refugee data. From an organisational point of view such controlled access supports accountability by clarifying responsibilty and purpose of access even when the data itself is accessed as a set rather than at the level of individual attributes.

5.5.3 Decentralisation and Avoidance of Unnecessary Data Accumulation

Another system level requirements concerns the avoidance of unnecessary data accumulation. Refugee perspectives stress the risks associated with large, centralised repositories of sensitive information while NGOs express awareness of the ethical and operational burdens of maintaining extensive datasets that exceed analytical capacity. These concerns align with critiques in the literature regarding 'data hubris' in humanitarian contexts.

The combined need point toward data practices which minimise aggregation and retain information close to it's source. Rather than collecting and storing data for potential future use systems should support access which is context specific and justified.

5.5.4 Transparency, Accountability and Traceability

Transparency emerges as a cross cutting requirement linking refugee trust and organisational legitimacy. Refugee prioritise knowing how their information is used and by whom while NGOs require clear accountability structures to show ethical compliance. Systems which lack transparency risk issues with trust on both sides.

A system level requirement thus emerges for traceability of data access and use. Transaparency supports refugee agency by making data flows visible and understandable and it supports NGOs by providing clear records of access decisions. This shared need reinforces the idea that ethical safeguards are not just constraints but conditions for sustained engagement and legitimacy.

5.6 Synthesis

This chapter examined the needs and priorities of refugees and NGOs in relation to data recording, sharing and analysis. The examination has stressed that emergency data practices are shaped by ethical, social and operational considerations. Refugees prioritise protection from harm, control over personal information, trust, accessibility while NGOs require structured, interoperable information which supports coordination,a accountability and identification of patterns across incidents.

A key insight that emerged is that refugee protection and organisational effectiveness are highly interdependeny. Refugee agency, privacy and trust are not barriers to humanitarian responses but prerequisites for meaningful and reliable data collection. When systems respect autonomy and minimise risk refugees are more likely to document their experiences.

At the same time the analysis shows that NGOs face constraints in the absence of structured and interoperable data. Fragmentation, inconsistent reporting formats and limited analytical ability obstruct the ability to detect repeating risks and respond proactively. Ethical responsibilty extends not just to how data is collected but also how it is accessed, interpreted and used.

Synthesising these perspectives lead to overarching implications for system design. Emergency data systems in refugee contexts must support privacy and data minimisation, enable meaningful consent and control, accommodate linguistic and situational diversity. Simultaneously they must provide NGOs with access to structured information which can be analysed to reveal patterns without compromising refugee safety.

The findings of this chapter set a clear foundation for the next chapter. The needs and priorities identified are translated in the following chapter into concrete functional and non functional requirements which define how a refugee centered emergency data system should be designed.

Chapter 6

System Requirements and Design Specifications

6.1 Introduction

This chapter talks about the second research question: What are the functional and non functional specifications required for designing a solid based emergency reporting system that meets the identified needs while safeguarding privacy, consent and digital agency?

The purpose of this chapter is to build on the needs and priorities (empirical findings) identified in chapter 5 and translate them into system requirements and design specifications. These specifications tell what a system should support so as to respond properly to ethical, social and operational challenges in refugee data context. Chapter 5 spotted recurring concerns relating to data control, selective disclosure, transparency of access, multilingual accessibility and need for structured, interpretable information.

To provide clarity the chapter differentiates between 3 layers of specification. first a set of design principals is articulated. These principals are obtained from needs identified in chapter 5 and existing literature. second functional requirements mention the concrete capabilities that the system should provide so as to support emergency data recording, consent management and analysis. third non functional requirements state quality attributes like privacy, security and usability.

6.2 From Identified Needs to Guiding Design Principals

The system requirements stated in this chapter are derived from empirical findings talked about in chapter 5 where interviews with refugees and NGO representatives showed repeating concerns relating to control over personal data, risks of misuse and need for structured information exchange. Instead of translating into isolated technical features the spotted needs were first synthesized into set of guiding principals. These principals function as intermediaries between stakeholder concerns and system level specifications. These principals establish ethical and conceptual foundation which shape functional and non functional requirements. Instead of motivating technical solutions they focus on the values and priorities which the system should

uphold so as to remain aligned with humanitarian context and realities faced by refugees and NGOs.

3 core principals structure the design of system:

1. Refugee Agency as foundational
2. Ethical Data Practices and principal of 'Do No Harm'
3. Balancing protection with humanitarian effectiveness.

6.2.1 Refugee Agency as a Foundation Principal

Chapter 5 showed that refugees continuously stresses importance of maintaining control over who can access tehir information. Concerns regarding involuntary data sharing and loss of control were central themes in interviews.

So refugee agency is treated as not an optional feature but a structural design constraint. From a specification perspective it implies:

- All interactions involving refugee data must be voluntary and initiated through explicit user action.
- The system should avoid assumptions of default consent or automatic data sharing.
- Users must be able to modify, revoke or discontinue participation at any time.
- System should provide clear visibility to what information exist and who can access it.

The principal informs requirements relating to explicit consent granting, revocability of permissions, separation of recording and sharing and visibility into active permissions and access events.

6.2.2 Ethical Data Practices and the Principal of 'Do No Harm'

The interviews talked in chapter 5 stress risk linked with repeated registration, exposure of sensitive information and possible misuse by institution. Emergency data systems operate in places where misuse, overexposure or misinterpretation of information could lead to serious consequences. This principal requires that data handling practice minimize risk. NGOs also acknowledge that existing practice may retraumatize refugees by asking them to again and again recount personal experience.

In humanitarian research such risks are framed under principal of 'do no harm' [5]. From a requirements perspective this implies:

- Data collection must be limited to necessary information for emergency support
- Data access events must be transparent and traceable.
- Architectural choices should avoid centralization of sensitive records.

- Default system state should minimize disclosure.

These directly inform non functional requirements like confidentiality, privacy by default, data minimization and transparency of access events.

6.2.3 Balancing Protection with Humanitarian Effectiveness

While safeguarding agency and privacy is important it was noted in chapter 5 that the emergency data systems should also support NGOs with structured, analyzable information to provide assistance, identify risks and coordinate responses. Fragmented and unstructured data limits effectiveness. Treating protection and effectiveness as opposite goals risk both.

This create a design tension excessive information risks harm while insufficient structure limits usefulness.

The third guiding principal thus tries to make balance between protection and operative effectiveness. The system should allow NGOs to understand and analyze data meaningfully without needing centralized ownership or unrestricted access. This implies:

- Incident data should be structured and semantically consistent.
- Authorized organizations should be able to filter and group records.
- Comparative analysis should be supported.
- Interoperable, standardised representation should be used.

By embedding structure a level of semantic modeling while preserving decentralised storage and user controlled access the system aims to sustain trust and practical utility.

6.3 Functional Requirements

Building on guiding principal talked in section 6.2 this section lists the functional requirements which define what the system must be capable of doing. For clarity these requirements are grouped into 3 categories:

- Refugee side functionality
- Consent and access control
- NGO side functionality

6.3.1 Requirements for Refugee Side Functionality

Given the sensitivity of the information included and the different circumstances under which refugees may interact with the system the following requirements define the minimum capabilities necessary for refugee participation:

FR 1: Structured Emergency Incident Recording

The system should allow users to record emergency incident in a structured format. Incident records should have clearly predefined field for important attributes like location, situation and expressed needs. Structured recording is important to ensure that information can later be interpreted properly.

FR 2: Optional and Incremental Data Disclosure

The system should allow users to provide information incrementally and selectively rather than forcing complete disclosure in a single interaction. Mandatory fields should be limited to that is necessary to create a valid incident record. Users should be able to omit or update information as circumstances allow recognizing that emergency situations often include stress, time pressure or safety concerns.

FR 3: Support for Additional Languages

The system is better if it supports interaction in multiple languages relevant to the target refugee populations. All core functions like data entry, system messages and consent related information should be available in supported languages to ensure understanding. Chapter 5 stressed importance of language accessibility for informed participation and meaningful consent.

FR 4: Clear User Feedback and Interaction Transparency

The system should give clear feedback to users during all stage of interaction like confirmation of saved records, indication of required/mandatory fields and acknowledgement of user actions. Feedback mechanism should be designed so as to reduce uncertainity and stress by making system behavior predictable and understandable.

FR 5: Location Capture upon Request

The system should allow optional capture of geographical coordinates via explicit user interaction. As concern relating to surveillance and exposure were raised in chapter 5 location retrieval should never occur automatically. The user should initiate GPS request ensuring location sharing remains consent based.

FR 6: Ability to Attach Supporting Evidence

The system should permit users to link supporting materials like images or documents wherever appropriate. Evidence attachment thus must stay optional and not be required/mandated for record creation. This requirement identifies that though supporting materials could strengthen documentation not all users will be able or will be willing to provide such evidence safely.

FR 7: User Visibility into Recorded Information

The system should allow users to view the information that they have provided. Users should be able to see their own records to ensure accuracy and completeness and to understand what

information exists within the system. This requirement supports agency and reduces the risk of unintentional disclosure.

6.3.2 Requirements for Consent and Access Control

The principal of refugee agency discussed in section 6.2.1 requires that data sharing should be governed by explicit, revocable and transparent consent mechanism. Chapter 5 showed concern about involuntary disclosure, lack of visibility into data flow were central to refugee viewpoint of digital systems. The following functional requirements define how the system must manage access to refugee data in a voluntary and transparent manner:

FR 8: Explicit Granting of Organisational Access

The system should require users to explicitly decide which organisations are authorised to access their emergency data. Access must not be granted by default and no organization should be able to see refugee data without a deliberate user action.

FR 9: Revocability of Access Permissions

The system should allow users to revoke previously granted access permissions at any time. Revocation should take effect without delay and not require justification.

FR 10: Separation between Data Recording and Data Sharing

The system should clearly separate the act of recording data from the act of sharing the data with organizations. Users should be able to create and maintain incident records without automatically sharing them to third parties.

FR 11: Role Based Access Differentiation

The system should differentiate between refugee and NGO roles. Each role should have access only to functionalities relevant to it's responsibilities.

FR 12: User Visibility into Active Access Permissions

The system should provide users with an overview of which organizations currently have access to their data. This must be understandable without technical expertise and must allow users to manage their active consent relationships.

FR 13: Transparency of Data Access Events

The system should make data access events visible to users indicating when an organisation has viewed their data. This supports accountability and reassures user that access to their data is traceable rather than being opaque.

6.3.3 Requirements for NGO Side Functionality

So as to support effective humanitarian response the system should provide NGO side functionality which allows authorised organisations to interpret and analyse refugee emergency data responsibly. Chapter 5 showed that humanitarian organizations need structured, interpretable information to assist effectively.

FR 14: Access to Authorised Refugee Records

The system should allow organisations to access refugee emergency records only when they have been explicitly authorized to do so. Access must be limited to data associated with established consent relationships and must not extend to unauthorised or unrelated records.

FR 15: Structured Presentation of Incident Information

The system should show authorized incident data to organisations in a structured and interpretable format. Incident attributes should be clearly labelled and organized to support quick understanding without needing technical expertise in data interpretation.

FR 16: Filtering and Grouping of Incident Records

The system should allow organisations to filter and group authorised incident records based on relevant attributes like location, date range, type of incident, expressed needs etc. This is important to support the identification of repeating risks, trends or clusters that might not be visible at the level of individual cases.

FR 17: Support for Pattern Identification and Comparative Analysis

The system should support comparative analysis across multiple authorized records so as to reveal patterns which could inform humanitarian decision making.

6.4 Non Functional Requirements

While functional requirements state what the system must do non functional ones specify the qualities and constraints which govern how these functions should be realized.In humanitarian emergency data contexts non functional requirements are very important as failures related to privacy, security or misuse could result in significant harm.

6.4.1 Privacy and Security Requirements

Privacy and Security constitute the foudational non functional requirements for any system handling emergency refugee data. Given the sensitivity of the information included the system should be designed to minimize exposure, prevent unauthorized access and reduce the potential impact of misuse.

NFR 1: Confidentiality of Refugee Data

The system should ensure that refugee emergency data remains confidential and inaccessible to unauthorized parties. Data must be only accessible to data subject and to organisations which have been explicitly authorized.

NRF 2: Privacy by Default

The system should adopt a privacy by default structure in which no emergency data is shared unless an explicit user action allows access. Default system states should favour non disclosure allowing that users are not required to opt out of data sharing.

NFR 3: Minimisation of Data Exposure

The system should minimise the amount of personal information exposed during normal operation. Data access should be limited to what is necessary for authorized purposes.

NFR 4: Semantic Consistency and Standardized Representation

All structured data should conform to predefined semantic schema aligned with controlled vocabularies and Common Data Model (CDM). Each input field should correspond to a clearly defined ontology term.

NFR 5: Interoperability

The system should use open standards for data representation and exchange to allow compatibility . Interoperability guarantees structured information could be integrated, analyzed and reused without requiring centralized storage mechanism.

NFR 6: Decentralized Data Architecture

The system should avoid centralized storage of refugee data. Information should remain within user controlled environments and querying mechanism should not aggregate central databases.

6.4.2 Usability and Accessibility Requirements

These are important non functional requirements for emergency data systems intended for refugee contexts. If a system is difficult to understand it risks excluding users.

NFR 7: Clarity of Language and Communication

The system should use clear, non technical language in all user facing communication including labels, instructions and feedback messages. Terminology should be consistent and understandable to users without specialized technical knowledge.

NFR 8: Accessibility Across Varying Levels of Digital Literacy

The system should be usable by individuals with varying level of digital literacy. Interaction patterns should rely on familiar and intuitive elements instead of requiring advanced technical skills.

6.5 Realisation of Requirements in the Prototype Architecture

The functional and non functional requirements defined in section 6.3 and 6.4 tell what the system should achieve and under which constraint. This section tells how these specifications are considered in prototype architecture of **Emergency Diary: My Secure Data Place**.

6.5.1 Decentralized Storage Model Using Solid Pods

To implement NFR1 (Confidentiality), NFR2 (Privacy by Default) and NFR6 (Decentralized Architecture) system adopts a decentralized storage model based on solid pods.

Each refugee's emergency data is stored within their personal solid pod. No central database aggregate incident record. This architectural decision operationalizes:

- FR8 (Explicit Granting of Organizational Access)
- FR9 (Revocability of Access Permission)
- FR10 (Separation between Data recording and Data Sharing)
- NFR6 (Decentralized Data Architecture)

6.5.2 RDF Based Semantic Data Modeling and CDM Integration

To satisfy FR1 (Structured Incident Recording), FR15 (Structured Representation), NFR4 (Semantic Consistency) and NFR5 (Interoperability) all incident data is presented using RDF.

Each input field in refugee interface is mapped to a corresponding ontology term and associated controlled vocabularies. This ensures:

- Machine readable structure
- Semantic Clarity
- Consistent representation across records
- Compatibility with SPARQL querying

Free text confusion is minimized by using predefined categories where appropriate. Also this semantic modelling approach realizes:

- NFR3 (Data Minimization)
- NFR 4 (Standardized Representation)
- FR16-FR17 (Filtering and Comparative Analysis)

6.5.3 Consent Enforcement and Access Control Mechanism

The consent framework defined in FR8, FR9 is enforced via webid based access control in the solid ecosystem.

Refugees grant access by specifying an NGO's webid. Permissions are directly written to access control layer linked with relevant RDF resources in user's pod. Revocation removes these permissions.

This mechanism operationalizes:

- FR8 (Explicit granting of access)
- FR9 (Revocability)
- FR12 (Visibility of active permissions)
- NFR2 (Privacy by Default)

Access transparency (FR13) is supported via a notification where refugees are informed when authorized organizations access their records.

6.5.4 Federated Querying Architecture using Comunica

To implement FR16 (Filtering) without violating NFR6 (Decentralization) the system integrate comunica federated SPARQL query engine.

Query execution occur over distributed endpoints and no central database is created.

This allows:

- Structured filtering across attributes
- Pattern identification across authorized records

While preserving:

- Decentralized storage
- Consent bound access

6.5.5 NGO Interface and Data Visualization Layer

To increase interoperability and usability the NGO dashboard present authorized records in tabular form and support dynamic visualization of query results.

Query outputs can be transformed into summaries generated from SPARQL result. These visualization help NGOs in spotting trends and comparative patterns without needing advanced technical expertise.

This layer strengthens:

- FR15 (Structured Presentation)
- FR17 (Comparative Analysis)

6.5.6 Multilingual and Interaction Design Safeguards

To support FR3 (Multilingual Interface) the system provides dynamic language switching between English and Tigrinya.

Interface safeguards include:

- Clear distinction between mandatory and optional fields
- Explicit confirmation messages for saving record
- Minimal free text reliance

Location capture (FR5) is implemented as an optional action. GPS retrieval occur only on explicit request and never automatic. Evidence upload (FR6) is stored directly within user's pod.

6.6 Alignment with FAIR OLR Principals (Ownership, Localisation and Regulatory Compliance)

Building on FAIR-OLR framework introduced in section 2.4 this section evaluates how the proposed system architecture aligns with governance dimensions of Ownership, Localisation and Regulatory Compliance. The analysis shows extent to which the design operationalizes these principals in refugee data context.

6.6.1 Ownership

The proposed emergency reporting system align with the ownership principal via:

- User controlled data storage in personal solid pods
- Explicit granting of access to NGOs (FR8)
- Revocability of active permissions (FR9)
- Visibility of active permissions and access events (FR12-FR13)

Data ownership is operationalized structurally where refugees retain control over who can access their incident records and no default sharing occur.

6.6.2 Localisation

The system described in this thesis aligns with the localisation principal via the following design choices:

- Incident data remains stored within refugee's solid pod
- No central database aggregates or replicates personal records
- Federated querying is used instead of data export

Data is thus not transferred to central repository for analysis. Instead authorized NGOs access data via federated mechanism consistent with the localization dimension described in FAIR OLR.

6.6.3 Regulatory Compliance

Regulatory compliance in refugee context is complex due to mobility of displaced populations. So the system cant assume alignment with a single regulatory framework. Instead of embedding compliance with a particular regime the architecture is designed to stay adaptable to applicable data protection laws of jurisdiction in which data is stored. Although the system is not deployed within a specific national regulatory framework its architectural logic support regulatory compliance via:

- Explicit consent based access control
- No automatic data transfer across jurisdictions
- Decentralized storage under user control
- Transparent logging of access events

These mechanism do not prescribe a specific legal framework but give structural condition under which compliance with varying national data protection regime can be operationalized.

6.7 Synthesis

Building on empirical findings presented in chapter 5 this chapter has translated the needs and priorities identified in chapter 5 into a nice set of system requirements and design specifications. Refugee priorities relating autonomy, consent and protection were formalized into design principals and consent centered functional requirements. NGO priorities relating structured information, filtering capabilities and comparative analysis were translated to controlled, semantically consistent analytical functionalities.

The resulting specification framework is organised into 3 layers: guiding design principals, functional requirements and non functional constraint. Together these define behaviour of system and conditions under which that behaviour should operate. Privacy by default, decentralized storage, semantic interoperability and explicit consent management are not optional features but structural conditions placed in architecture.

Section 6.5 showed how these requirements can be realized technically via decentralised solid pod storage, RDF based semantic modelling, federated querying and user controlled access mechanism. Section 6.6 further situated the system within FAIR OLR framework showing alignment with principals of ownership, localisation and regulatory compliance in sensitive data environments.

Chapter 7

System Implementation and Deployment

7.1 Introduction

This chapter talks about the third sub research question: How can such a system be implemented and deployed in a technically feasible manner that meets the identified specifications?

Building on the requirements spotted in chapter 6 this chapter shows the realization of system and explains how it's core components have been implemented. While the previous chapters talked about needs, principals and requirements this chapter describes the implemented architecture. The aim is to show how the specified functional and non functional requirements were translated into a working application which supports refugee centered data recording and controlled humanitarian access.

7.2 Architectural Overview

The developed system follow a decentralized, web based architecture which separates data storage, access control and application logic. This approach of architecture shows the decision to avoid centralized repositories of sensitive refugee data while still allowing authorized organizations to access and analyze information when permission is given.

At a high level the architecture has 3 main components: first is the refugee controlled solid pods for data storage; second is the web based application which gives refugee and NGO interfaces and third is the authorized access mechanisms which tell how organizations retrieve and process data.

The decentralized and browser based nature of the system assumes that users interact via a personal digital device capable of web authentication and securer session handling. While this align with increasing digital access in humanitarian contexts availability of personal devices cant be uniformly assumed in displacement settings.

7.2.1 Decentralized Architecture Based on Solid Pods

The system uses solid pods as the main storage mechanism for refugee's emergency data. Every refugee stores their records within their own solid pod guaranteeing that data remains under the power of the individual user rather than being sent to a central server. The application itself doesnt maintain a database of refugee information instead it reads from and writes to user controlled pods based on authenticated sessions and access permission.

This decentralised storage model means that sensitive data is distributed across individual pods instead of being aggregated in single location. From an implementation point of view the application interacts with solid pods using standard solid libraries performing authenticated read (or write) operations. Access to these resources is controlled by solid's access control mechanisms which decide which organization are permitted to retrieve data.

7.2.2 Role Separation: Refugee and NGO Interfaces

Although it is implemented as a single web application the system supports 2 different roles: refugees and NGOs. Role separation is handled at the level of application with different interface flow and functionalities presented depending upon the authenticated user's role.

Refugees interact with the system to record emergency data, manage consent and see which organizations have access to their data. NGO users on other hand are given with interface which allow them to retrieve and analyze incident data for which they have been authorized. This separation ensures each group of user is presented only with functionality relevant to their role reducing complexity and likelihood of misuse.

7.2.3 Data Flow Across the System

The flow of data within the system follow a clear sequence. Refugees authenticate using their solid Webid and record emergency data via the web interface. The application serializes this information into a structure format and stores it inside refugee's solid pod. At this point the data stays private and inaccessible to third parties.

When a refugee gives access to an NGO the applicate updates access control settings. Authorized organizations could then retrieve permitted data from refugee's pod. Retrieved data could be queried and aggregated by the NGO facing components of the application without copying into a central database.

As the system relies on solid based authentication and real time interaction with individual pods it's operation needs active internet connectivity. While this model allows decentralization and dynamic consent control it also mean that the system cant function in offline conditions.

7.3 Data Modelling and Semantic Representation

An important aspect of the system design is the use of semantic data modelling to present emergency data in a structured, interoperable and machine readable form. Instead of storing

emergency information as unstructured text the system represents data using RDF (Resource Description Framework) allowing consistent interpretation and flexible querying.

7.3.1 Emergency Incident Representation Using RDF

Emergency incidents recorded by refugee are presented as RDF resources stored within their solid pods. Each incident is identified by a unique identifier. Representing incidents in RDF allows the system to capture relationship between entities.

When a refugee submits emergency data through the app interface the data is serialized into RDF triples and stored in turtle format within user's pod. RDF supports extensibility and semantic clarity allowing additional attributes to be introduced without breaking the existing data structures.

7.3.2 Use of a Common Data Model (CDM)

To ensure consistency between records the system uses a CDM which defines the classes and properties used to describe emergency situations. The CDM gives a shared semantic structure for representing incidents, victims, locations etc reducing ambiguity.

In the system, the CDM acts as semantic contract between data producer and data consumer. Recorded incidents conform to the CDM enabling NGOs to interpret data uniformly regardless of the individual.

7.3.3 Ontologies, Controlled Vocabularies and Semantic Consistency

Building on semantic modelling principals outlined in section 2.6 the system incorporate ontologies and controlled vocabularies to ensure consistent representation of emergency incidents. Where appropriate values like incident type, country or category are presented using predefined terms instead of free text input. This supports consistent understanding across records.

Ontology files in the application are used to enrich the semantic context of recorded data. By combining RDF, CDM and controlled vocabularies the system gets a balance between structure and flexibility.

7.4 Refugee Side Implementation

The refugee side part of the system is designed to allow individuals to safely record emergency information and interact with the system in a manner which is accessible under stressful conditions. This section tells how refugee side functionality is implemented in practice.

The refugee interface is implemented as web based application which runs entirely in user's browser and interacts directly with the user's solid pod. All actions performed by refugee like recording incidents or managing access permissions are performed within the context of user's authenticated session ensuring control over data remains with the individual.

7.4.1 Authentication and Identity via Solid WebIDs

Refugees authenticate to the system using their solid webid which acts as a decentralized identifier linked to their solid pod. Authentication is handled via Solid OpenID Connect (OIDC) enabling users to log in through their chosen solid identity provider. Upon successful authentication the application establish a session which enables read and write access toi the user's pod according to the permissions granted by the provider.

The use of webids ensure that application does not manage or store credentials itself. Instead identity management is handled by solid ecosystem reducing security risk and allowing refugees to reuse an identity they already control. Once authenticated the application retrieves the base pod location associated with the webid and uses it as the storage context for emergency data.

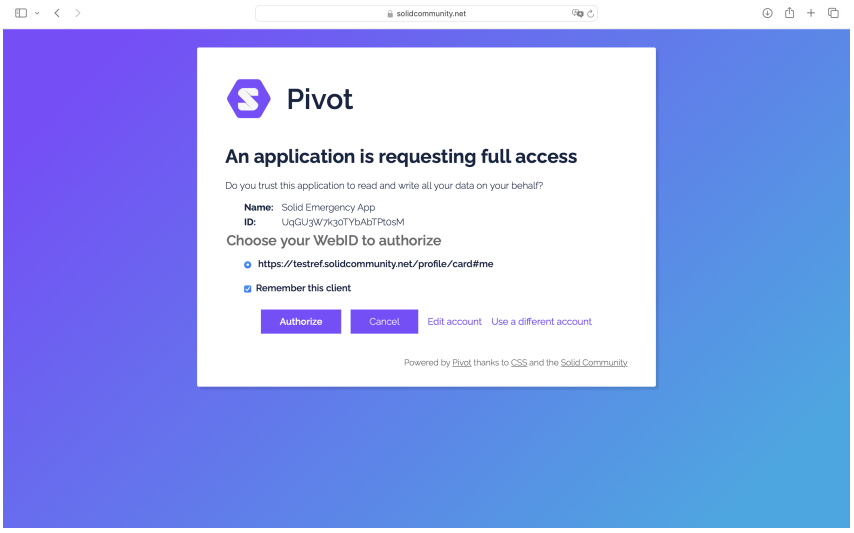


Figure 7.1: Authentication via Solid WebIDs

7.4.2 Structured Emergency Data Entry

After authentication refugees could record emergency information through a structured form based interface. Mandatory fields are limited allowing refugees to submit partial information when circumstances do not permit full disclosure.

Form parts like dropdown menus, checkboxes and text fields are used to reduce ambiguity and support consistent data interpretation. At the same time the interface allows flexibility by allowing users to skip non essential fields.

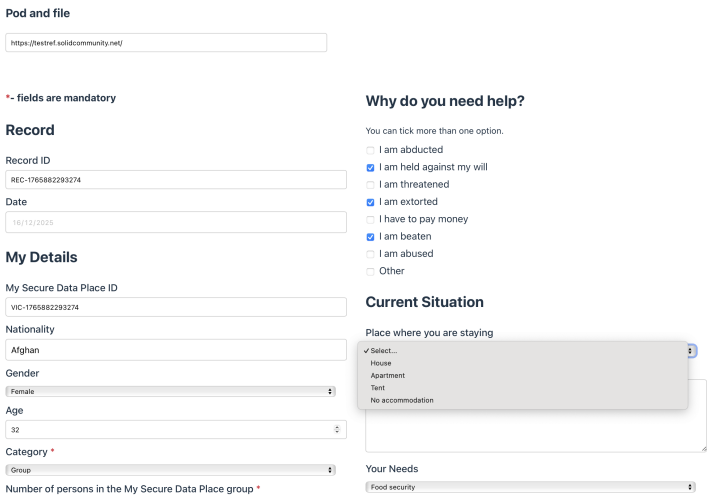


Figure 7.2: Structured Emergency Entry

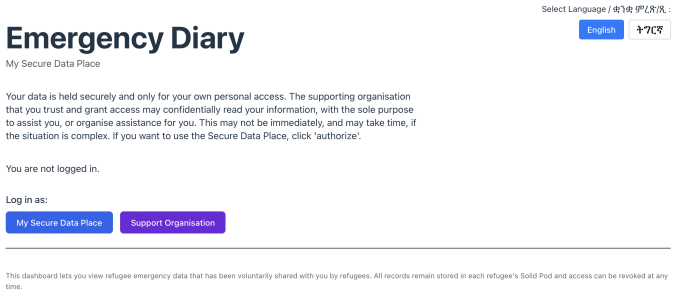
7.4.3 Language Support and Accessibility

The refugee interface supports interaction in 2 languages to improve accessibility and understanding. At present the system offers interfaces in English and Tigrinya allowing users to switch languages directly within the application. Language selection affects all user facing text including form labels, instruction, system messages and consent related information.

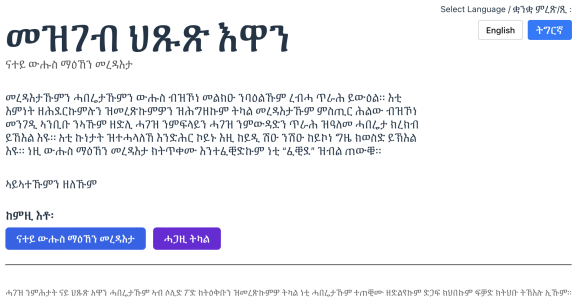
To guarantee accuracy of Tigrinya interface the English user facing text including labels, instructions and consent messages was first compiled into a text file. This file was shared with Mr. Danial Zemschal Tesfahans (Lecturer and Researcher at Aksum Univeristy, Ethiopia) who provided corresponding Tigrinya translations. The translated terms were integrated into application interface. This guaranteed that language adaptation reflected native understanding rather than automated translation.

Language switching is implemented dynamically allowing users to change language without restarting the session or losing entered data. This guarantees that refugees can interact with the system in their preferred language which is important for understanding sensitive information and making informed decisions.

However refugee populations are linguistically diverse and broader deployment would need expanded multilingual integration. While bilingual support shows feasibility comprehensive language coverage reamain a necessary extension for large scale applicability.



(a) Login screen (English)

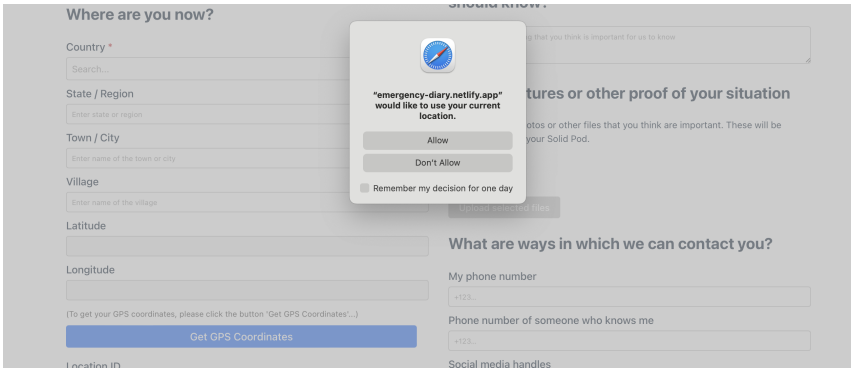


(b) Login screen (Tigrinya)

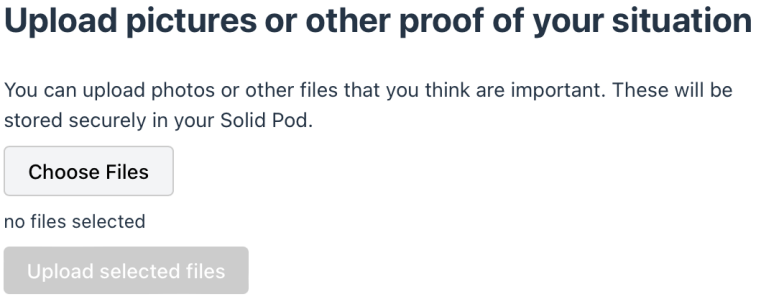
7.4.4 Optional Location and Evidence Handling

The system allows refugees to optionally give information like geographic location and supporting evidence. Location data could be captured using the device's GPS functionality based on user's consent. When enabled latitude and longitude coordinates are fetched via the browser's geolocation API.

In addition to this the refugee may optionally attach supporting materials like images or documents. Evidence submission is never mandatory and clearly presented as optional. This design acknowledges that giving such information might not always be safe and ensure that user are not pressurized to disclose additional data.



(a) Linking Location



(b) Linking Evidence

7.5 Consent and Access Control Implementation

Consent and access are implemented as the core functionalities which govern how refugee emergency data is shared with authorised organizations. Instead of treating consent as an external policy or static agreement the system places access control directly into the application.

All consent related actions are done by refugee via the application interface and at level of solid pod resources. As a result access control is not mediated by the application alone but is reflected in permissions linked with data itself.

7.5.1 Private by Default Data Storage

When a refugee records an incident the data is stored in their solid pod with no organizational access enabled by default. Newly created records are only accessible and visible to the subject guaranteeing that information remains private unless the refugee chooses themselves explicitly to share it.

This private by default behaviour is done using solid pod's access control mechanism. From the user's point of view this means that recording an incident does not mean immediate sharing allowing refugees to document situations safely without disclosure commitment.

7.5.2 Granting and Revoking NGO Access

The system offers refugees with a dedicated interface for managing access to their emergency information. Refugees could add NGOs by specifying their WebIDs and explicitly grant access to their records.

Once access is given the authorized NGO could retrieve refugee's data from solid pod. Importantly the system allows refugees to revoke access at any time. Revocation instantly removes the organization's ability to access the data without requiring confirmation from the NGO. Access management is made simple where refugees could add, remove NGOs from their authorized list via a single interface.

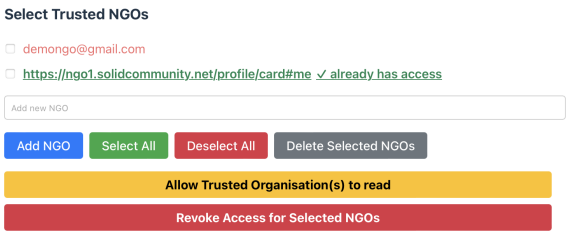


Figure 7.5: NGO Addition and Access Grant (or Revoke)

7.5.3 Access Transparency and Visibility

Refugees can view which NGOs have permission to access their emergency data allowing them to assess and manage active consent relationships at any time.

When an NGO queries refugee data this interaction is logged and made visible to the data subject. This ensures that access is not vague and reinforces accountability by making organizational interaction traceable.

7.6 NGO Side Implementation

The NGO side component allows authorized organizations to retrieve, understand analyze emergency data shared by the refugees. The NGO interface is inclined toward responsible data access and pattern identification.

NGO users authenticate using their own solid webids. Their ability to view data is constrained by the access permission set by refugee. At no point the system give NGO visibility into data for which they have not been authorized.

7.6.1 Auhtorized Data Retrieval

When an NGO access the system the application authenticates the user via their solid webid and tells which refugee pods they are authorized to access. Authorization is verified by checking the access control settings linked with the relevant pod resources. Only the data explicitly shared with NGO is retrieved and showed.

Data retrieval is done directly from the refugee pod instead of an intermediate server or a central database.

Figure 7.6: Authorized Access

7.6.2 Federated Querying and Aggregation Using Comunica

So as to support analysis across multiple data sources the system uses federated querying using the comunica framework. It allows the execution of SPARQL queries over distributed RDF sources allowing application to query multiple refugee pods simulataneously and that too without consolidating data into a central repository.

The application makes SPARQL queries which are executed over all authorized pods linked with an NGO. Query results are aggregated to produce combine view of incident data like grouped includes by location or data etc.

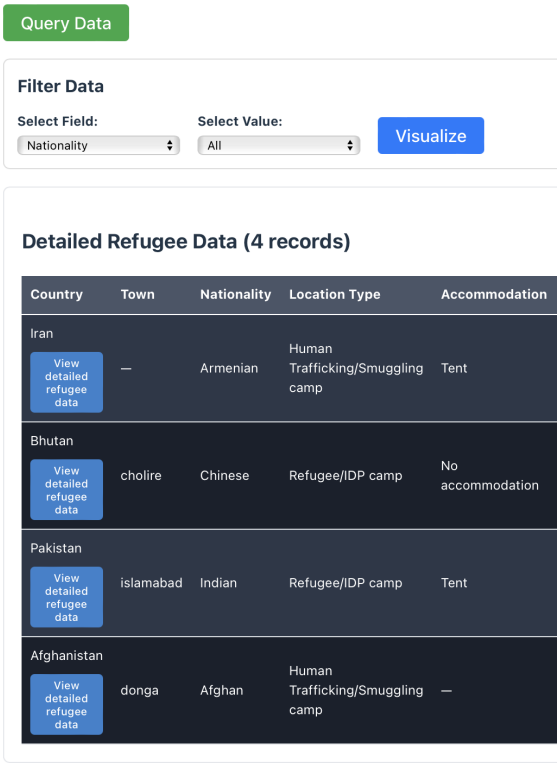


Figure 7.7: Query Results

7.6.3 Pattern Identification

Visual representations in the form of a pie chart are used to support understanding without overwhelming users. The focus is on clarity instead of exhaustive analytics reflecting the system's focus on responsible use of sensitive data.

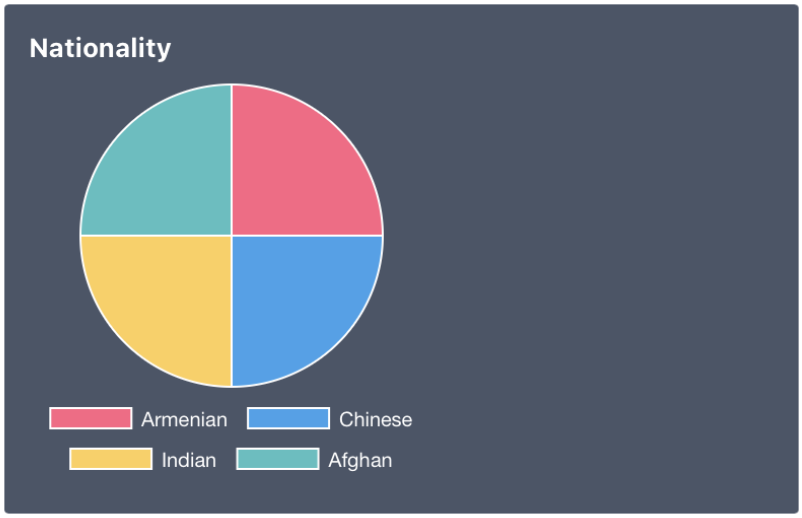


Figure 7.8: Visual Results

7.7 Deployment

In addition to the system implementation the application has been deployed to show technical feasibility and real word usage. Deployment was done with focus on emphasis on simplicity guaranteeing that the system could be accessed by users wihtout needing specialized infrastructure.

The deployed system is publicly accessible as a web application at:

`https://emergency-diary.netlify.app`

7.7.1 Deployment Strategy

The system is deployed as a static web app with all client side logic executed within the user's browser. This strategy aligns with the system's decentralized architecture as no refugee data is stored or processed on the hosting server. The application interacts directly with solid pods via authenticated requests.

The deployment strategy ensures that system availability is independent of the data ownership. Refugee data remains stored within individual solid pods while the deployed application works just as an interface for interaction and authorized access.

7.7.2 Continuous Deployment via GitHub and Netlify

the source code of the application is maintained in a private github repository. Deployment is managed via integration with Netlify which is designed to automatically build and deploy the application whenever changes are pushed to the repository.

Netlify pulls the source code from the github repository and executes the process. Keeping the repository private also minimizes the risk of unintentional exposure of implementation details while still letting the deployed application to be publicly accessible.

This pipeline supports refinement of the system enabling improvements to be made incrementally in response to feedback.

7.7.3 Current Deployment Status

At the time of writing the application is fully deployed and accessible online. Users could authenticate using solid webids, record emergency incidents, manage access permissions and retrieve authorized data via the deployed interface. Deployment confirms that the system is not limited to an experimental setting but can operate in a real world environment.

7.8 Synthesis

This chapter has talked about the implementation and deployment of a refugee centered emergency data system. The system has been realized as a decentralized, web based application which allows refugees to record information, manage consent and retain control over their data while allowing humanitarian organizations to retrieve and analyze information.

The chapter discussed the system architecture stressing the use of solid pods for user controlled data storage. It explained how emergency incidents are modeled using semantic representations allowing structured and interoperable data exchange without depending on centralized databases.

The chapter also discussed how NGOs can retrieve authorized data via federated querying without compromising refugee agency. The deployment strategy showed that the system is technically feasible and operational as a publicly accessible web app supported by an automatic deployment pipeline.

Chapter 8

Adoption Potential

8.1 Introduction

This chapter talks about the fourth sub research question: What is the potential for adoption of this system by refugees and NGOs considering usability, trust and ethical acceptability?

It present the empirical findings relating to adoption potential of proposed emergency incident reporting system. The analysis is structured according to Unified Theory of Acceptance and Use of Technology introduced in chapter 2.

The findings presented here are based on semi structured interviews conducted with 5 refugees and 2 NGO representatives listed in the table A.1. The interviews explored perception of usefulness, ease of use, trust, social influence, required conditions and overall intention to adopt the system. The full list of interviews is given in appendix A, the transcripts are included in appendix B and coding labeling spreadsheet used for thematic analysis is shown in appendix C.

The data was analyzed using thematic coding. These codes were grouped under 4 main UTAUT constructs: performance expectancy, effort expectancy, social influence and facilitating conditions. A final category behavioural intention synthesizes overall willingness to adopt the system.

The following sections present empirical findings construct by construct.

8.2 Performance Expectancy

It refers to the extent to which stakeholders believe that using the system will give meaningful benefits in practice. Within UTAUT framework this construct is strongest predictor of behavioural intention.

NGO Perspectives

From NGO perspective usefulness was closely linked to improve current documentation practices. NGO-B (Danial) describe a repeating problem in humanitarian context that refugees are frequently required to repeat their experience multiple times to different organizations. Repeated questioning was viewed as harmful and a more controlled documentation mechanism

was taken as beneficial. When reflecting on the emergency system presented during demonstration (appendix D) the same participant said:

"I think this application has potential to address this challenge." (Interviewee NGO-B, December 19, 2025) B

Here usefulness is directly linked to system's potential to solve a real structural problem. Within UTAUT logic such a recognition strengthen the likelihood that an organization would consider adopting the technology.

NGO-A (Makeda) A.1 also acknowledged the potential value of system because it centralizes information under refugee control while still allowing organizational access when authorized.

Refugee Perspectives

For refugee participants usefulness was mainly linked to control over personal information and improved access to support in emergency situations.

R2 A.1 stressed that system's value lies in safe storage and consent based sharing:

" *It only stores my information... and I know that it wouldn't be disclosed without my consent.*" (Interviewee R2, January 18, 2026) B

This indicates usefulness was not seen just as digital convenience but as protective of sensitive information. The ability to decide who sees data was repeatedly framed central.

R3 A.1 linked usefulness directly to emergency response:

" *It will enable the non-government actors to trace me and to provide humanitarian support for me.*" (Interviewee R3, January 18, 2026) B

In this case perceived usefulness is linked to being located and helped in critical situations. It demonstrates refugees assessed the system in terms of whether it could improve their safety and access to help.

A clear convergence came out across both stakeholder groups regarding system's usefulness. However a divergence can be seen in how usefulness is framed like NGOs stressed structural efficiency and harm reduction while refugees prioritized personal agency and safety.

8.3 Effort Expectancy

It refers to the degree to which stakeholders perceive the system as easy to use and comfortable to interact with. Within UTAUT framework perceived ease of use influence behavioural intention mainly in context where users may face cognitive, linguistic or technological barrier.

Refugee Perspectives

Across refugee interviews participants continuously described the system as clear and understandable. A key factor influencing this viewpoint was accessibility of language. One participant said:

"*Because it is present in my own language, Tigrinya, I feel that I can fill it fully, and for me it's simple.*"

This suggests ease of use wasnt assessed just in technical terms but also in terms of linguistic inclusivity. The availability of familiar language reduced perceived complexity.

Another refugee participant stressed that the system would be manageable also under stressful conditions:

"*It will enable the person to navigate a resolution while being in a challenging situation.*" (Interviewee R3, January 18, 2026) B

According to UTAUT effort expectancy is mainly impacted by age and experience. In this study all refugee participants including those aged 20-30, 35, 40-50 and 46 reported regular use of smartphones and banking applications (Ref-A, R1-R4) A.1. No participant expressed difficulty understanding the interface during demonstration. So digital familiarity contributed to a relatively low perceived effort.

NGO Perspectives

From NGO perspective effort expectancy was also positive. NGO-A (Makeda) A.1 expressed that the interface appears manageable for organizations at least on the face of it.

NGO-B (Danial) A.1 raised another important point concerning form length and time constraints. He noted refugees may not always be in a stable environment when filling in information:

"*If the questions are too much, then they may not have that much leisure time to fill it in.*" (Interviewee NGO-B, December 19, 20225)B.

This highlight that perceived effort is context dependent. While interface may be technically simple situational stress could increase perceived burden of use.

Given that no participant described the system as confusing or technically complex effort expectancy doesnt appear to be a barrier to adoption in this study.

8.4 Social Influence

It refers to the extent which stakeholders perceive that opinions, expectations or behaviors of others affect their willingness to use the system. Within UTAUT this construct capture the impact of peer endorsement, community acceptance on behavioural intention.

Refugee Perspectives

Several participants said that they would recommend the system to others. When asked whether he would recommend application to people travelling in similar situations one participant responded:

"*Yes, I recommend this application to be used by others as well.*" (Interviewee R2, January 18, 2026) B

Another participant similarly indicated willingness to recommend system:

"*Yes, I can recommend them.*" (Interviewee R3, January 18, 2026) B

These suggest social endorsement could develop organically within refugee communities if the system is perceived as trustworthy and beneficial.

One participant (R2 A.1) reflected on how others might respond if introduced to the system saying that he feels that others would accept this application as they are the only person who are accessing it. This suggest community acceptance is also linked to system's privacy and security nature. Within UTAUT logic such willingness to recommend and expectations of broader acceptance strengthen behavioural intention as individuals are more likely to adopt technologies perceived as socially validated.

NGO Perspectives

For NGO representatives social influence was more about institutional credibility and professional networks. NGO-A (Makeda) A.1 stressed implementation would require advocacy and organizational support. This suggests for NGOs adoption would depend not just on individual belief in usefulness but also on collective recognition within organization.

Similarly NGO-B (Danial) A.1 expressed that demonstrating practical value would be necessary before wider acceptance. This highlight that social influence in organizational context operates via processes like peer discussion and testing.

Both male and female participants expressed similar willingness to recommend the system.

A convergence could be observed that adoption is socially influenced instead of purely individual. However a divergence comes out at the level at which social influence works. Refugees framed it mainly in terms of peer recommendation and community acceptance whereas NGO representative stressed institutional legitimacy, piloting processes etc.

8.5 Facilitating Conditions

It refers to extent which stakeholders perceive that the necessary organizational, technical and infra support exist to enable use of the system.

Refugee Perspectives

For refugee participants facilitating conditions were mainly framed in terms of accessibility, affordability and guidance.

1 important issue raised linked to financial accessibility. When asked to a participant whether system should be free he responded:

"*There are some perceptions where people feel that it would be fake if it is for free, but in the context of Eritrean refugees in Ethiopia, they don't have access to economic means...it would be recommended to be provided for free.* "(Interviewee R2, January 18, 2026) B

This show that while cost may impact perceived credibility financial accessibility is important for actual adoption within vulnerable populations.

Training and guidance were also spotted as enabling factors. When asked whether support would increase willingness to use system one participant said:

"*Yes, it will boost my interest to use this application.*" (Interviewee R2, January 18, 2026) B

This show that facilitating condition like user orientation or demonstration could impact behavioural intention positively.

NGO Perspective

For NGO participants facilitating conditions were more strongly linked to organizational readiness. NGO A (Makeda) A.1 expressed that their organization has all the means and the facilitating conditions for this system as this system is not very demanding.

NGO- B (Danial) A.1 stressed the importance of piloting:

"*It needs to be piloted...checked through filling some data.*" (Interviewee NGO-B, Decmber 19, 2025) B

He also suggested that initial training relating to the application would be helpful for refugees. This show that organizational adoption also depend on validation processes and training and feasibility.

Within UTAUT framework these findings show that adoption depends on whether adequate support structures: financial, technical, institutional are in place.

A divergence could be seen where refugees stressed individual level enablers like affordability while NGO representatives focused on organizational readiness, piloting procedures etc.

8.6 Behavioural Intention

It refers to stakeholder's expressed willingness or openess to use the system taking into account perceived value, ease of use, social influence and facilitating conditions.

Refugee Perspective

Across refugee interviews participants continuously expressed interest in using the system. When asked directly from the participants whether they would use system in future all of them were enthusiastic and showed interest in actually using the application.

When asked about their perception on whether others would be willing to actually use this application a participant said:

"*I feel that many Eritreans in Ethiopia would want to use it.*" (Interviewee R2, January 18, 2026) B.

R2 A.1 also added:

"*I feel that they will accept this application fully because it stores their own information and they are the only person who are accessing it.*" (Interviewee R2, January 18, 2026) B

This shows not just personal willingness to adopt but also readiness to promote system within peer networks.

Another participant described broader applicability beyond emergencies:

"*Not only for humanitarian context, but to store my information as well...where I cannot feel safe to store it in other ways.*" (Interviewee R1, January 18, 2026)

This suggest that system is perceived as useful in both emergency and non emergency context.

NGO Perspective

Among NGO participants behavioural intention was also positive. They expressed that something like this doesnt already exist which supports refugees safely and also allows NGOs to provide support to them in a systematic and simple way.

Both NGO representatives expressed willingness to use the system but also expressed that some testing would help strengthen the trust in the system.

NGO-A (Makeda) A.1 indicated that the dual language availability in the system is good for initial testing and usage of the system but more languages could be added in the future.

In conclusion both representatives were happy with the system and said they would like to use this system.

8.7 Synthesis

This chapter examined the adoption potential of the developed system via lens of UTAUT. Drawing on empirical interview data from refugee participants and NGO representatives the analysis assessed performance expectancy, effort expectancy, social influence, facilitating conditions and behavioural intention.

Across the UTAUT constructs the interview insights shows that the system is taken as potentially useful particularly in relation to ethical data handling and refugee protection.

Performance expectancy came out consistently positive. Refugees saw the system as increasing personal security, consent based data sharing and emergency support. NGO representatives spotted improvements in documentation practices, reduction of repeated questioning and more structured information management.

Effort expectancy was also seen positively. Refugee participants described system as understandable and manageable mainly due to language accessibility and structured input options. NGOs also found the system easy to use.

Social influence appeared differently across groups. Among refugees willingness to recommend system and expectation of peer acceptance suggest community endorsement could facilitate adoption. Among NGOs institutional validation and professional advocacy were seen influential.

Facilitating conditions came as a very important decisive factor for sustained adoption. Refugees highlighted affordability and training as the main enabling conditions. NGOs stressed piloting, organizational readiness.

No big variation in perceptions was seen across gender or age groups within the sample. All refugee participants reported regular digital experience.

Overall the convergence of positive performance expectancy, manageable effort expectancy, supportive social endorsement and identifiable facilitating condition suggest the system has realistic adoption potential within both refugee and NGO context.

Chapter 9

Discussion and Conclusion

9.1 Discussion

This thesis studies whether a refugee centered emergency incident reporting system can be designed and implemented in a way which strenghtens refugee data agency while still allowing humanitarian organizations to spot meaningful patterns across incidents. Through the previous chapters we saw that many shortcomings in existing data practices are not entirely technical but ethical in nature. Interviews and literature showed refugees are often required to disclose sensitive personal information repeatedly without clarity regarding ownership, access or future use. At the same time NGOs see fragmented and inconsistent data which limit their ability to spot repeating risks like repeated detentions, ransome demands etc.

This discussion thus answer the sub questions (RQ1-RQ4) first before returning to overarching research question:

RQ1: Needs - What are the needs and priorities of both refugees and NGOs in relation to data recording, sharing and analysis?

The need analysis stressed a shared concern which is emergency information is valuable only when people are willing to and able to record it and willingness depends highly on trust, control and clarity.

From refugee viewpoint needs revolved around:

- Control and safety: a mechanism to record incidents without loosing control over who can see information.
- Informed consent: not just that consent exist but that user can understand what is shared, with whom and can revoke it.
- Language and understanding: the system should reflect realistic linguistic context otherwise consent becomes procedural instead of meaningful.

From NGO viewpoint needs focused on:

- Structured, comparable information: consistent field which allow searching and filtering across incidents.

- Pattern detection without unethical data accumulation: NGOs need to spot repetition but dont want to reintroduce large repositories which create ethical risks.
- Interoperability and analytical workflow: ability to work with data across cases.

RQ2: Specifications and Requirements - What are the functional and non functional specifications required for designing a solid based emergency reporting system that meets these needs while safeguarding privacy, consent and digital agency?

The requirements phase translated such needs into concrete system expectations.

Functional requirements involved:

- Structured incident entry
- Consent based access control
- Selective sharing
- Query capability for NGOs

Non functional requirements included:

- Privacy and security by design
- Transparency and accountability
- Usability under constrained conditions

RQ3: How can such a system be implemented and deployed in a technically feasible manner that meets the identified specifications?

This thesis showed technical feasibility via implementation of a functional prototype which combines:

- Decentralized storage
- Explicit permissioning
- Federated querying

A key implementation outcome is that decentralization doesnt remove possibility of organization insight instead it changes how insight is produced. Instead of bulk extraction into a single repository analysis becomes dependent on authorized access and federated computation.

RQ4: Adoption potential - What is the potential for adoption of this system by refugees and NGOs considering usability, trust and ethical acceptability?

Adoption was assessed via the interview data and the UTAUT informed analysis. Adotpion potential depended mainly on:

- trust and perceived safety

- how easy it is to understand and use
- device access, connectivity, language understanding
- wether system improve the ability of NGOs to spot patterns
- whether it can integrate without creating additional burden

Overall the adoption analysis suggest cautious optimism. The proposed model align strongly with ethical acceptability and might increase willingness to document and share.

9.2 Answering the Overarching Research Question

Overarching RQ: How can a refugee centered emergency incident reporting system be designed and implemented to empower refugees with control over their data while enabling NGOs to search, filter and interpret structured patterns in the reported data in a way that is both technologically robust and ethically aligned?

The finding of study suggest such a system is achievable when certain commitments are made simulataneously:

- Agency is embedded architecturally: decentralized storage guarantee emergency records are not institutionally owned by default reducing the structural imbalance which currently characterize humanitarian data systems.
- Consent becomes operational instead of symbolic: informed consent is implemented as set of concrete system action like explicit access granting, revocation and transparency, so control is exercized continuously instead of assumed at point of collection.
- Organizational insight is produced without central accumulation: federated querying allow NGOs to spot patterns across authorized records maintaining analytical value while avoiding governance risks of building another large scale dataset.

These result show that refugee agency and organizational effectiveness could be aligned. Systems which reduce perceived risk and increase clarity may lead to more complete reporting which improve data reliability and thus improve quality of humantiarian analysis and response.

9.3 Reliability and Validity

Reliability and validity are addressed in terms of trustworthiness and design research.

Reliability

- The study followed a documented procedure for data collection (semi structured interview), analysis (coding and convergence divergence) and translation of findings into requirements and implementation steps.
- The protoype development process was iterative and traceable via github creating a trail from needs to requirements to implemented features.

Internal Validity

- It was strengthened by comparing viewpoints across distinct stakeholders and by aligning interview derived themes with literature.
- The analysis wasnt aimed at quantifying frequencies but rather at spotting consistent themes which explain priorities, trade offs and adoption conditions.

External Validity

- The empirical case is bounded (Eritrean refugees in studied contexts) so findings should not be generalized statistically.
- However transferability is supported at level of design logic. The principal that consent based access, minimization and transparency can be built into infrastructure is relevant to other humanitarian setting where trust and governance failure limit data quality.

9.4 Limitations

Like any other thing or application there exists some limitations which were also mentioned in chapter 7:

- **Limited Language Support:** The current system supports interaction in only 2 languages. While this allows use by specific refugee groups (like in Eritrea as they speak Tigrinya) broader adoption will require support for additional languages like Arabic, French, Somali, Amharic etc to better reflect the linguistic diversity.
- **Dependence on Internet:** The application needs an active internet connection to authenticate users and interact with solid pods. This could be a constrain where connectivity may be unavailable.
- **Reliance on Access to Personal Digital Devices:** Use of the system assumes access to a smartphone or a personal device. Refugees without consistent access to such device may face barriers.

9.5 Future Directions

- A key area for future development is expanded multilingual support. Expanding language support will strengthen informed consent by ensuring that system prompts, access control and data sharing implications are properly understood by all users.
- Another important direction is regarding connectivity and offline resilience. Future iterations could explore mechanisms for offline or low connectivity usage. Such a functionality will help better align the system with realities of displacement and emergency contexts.
- From an organizational perspective future work could study deeper integration with humanitarian workflow. Careful consideration would be needed to make sure any integration doesnt reintroduce centralization.
- Additional aggregation or visualization features could support NGOs in spotting patterns more effectively given that these improvements respect the boundaries of authorized access.

9.6 Conclusion

This thesis set out to design and implement a refugee centered emergency incident reporting system which balance two goals often treated as competing: refugee control over emergency data and NGO capability to detect actionable patterns. Thorugh a combination of literature analysis, stakeholder need assessment, requiremtns translation, prototype implementation and adoption oriented evaluation the study shows that such goals could be aligned when decentralization, consent and transparency are treated as infrastructure features instead of policy aspirations.

Empirical findings show that refugees were mainly concerned with ownership, repeated disclosure of sensitive information and lack of transparency regarding who accesses their data. NGO representatives stressed need for structured, analyzable information to spot patterns across cases. The prototype showed these concerns are not mutually exclusive. Decentralized storage combined with explicit consent and federated querying could support both individual control and aggregated insight without centralizing of data.

The key takeaway is that ethical design choices can directly improve data usefulness. When refugees could understand and control sharing they are more likely to document incidents which improve the reliability and actionability of information for protection work. At the same time NGOs could still derive value via authorized federated querying instead of central extraction.

To the best of our knowledge this work represents one of the first practical implementations which combine decentralized data storage, explicit consent based access control and federated querying within a humanitarian emergency reporting context. The application gives a concrete example of how refugee agency can be fitted directly into data infrastructure.

This thesis also acknowldeges the limitations though they do not undermine the system but indicate that iterative improvement informed by user feedback would help even better the system. Looking forward this work suggests that decentralized, refugee controlled data systems have the potential to influence how humanitarian information is collected, shared and governed. Such systems could contribute to the bigger shift toward data practices which are not only effective but transparent and respectful of dignity.

Future research should explore large scale deployment across diverse refugee context to assess usability, adoption and long term trust effect. Further work is neede to develop offline resilient architectures suitable for unstable connectivity environment and to expand multilingual integration to reflect linguistic diversity in displacement settings.

Lastly this thesis argues building humanitarian technologies around refugee agency is both feasible as well as necessary. Doing so opens new possibilities for trust, accountability and sustainability in humanitarian data systems and gives a foundation for future research and innovation in this domain.

Bibliography

[1] D. Kaurin, "Data protection and digital agency for refugees," Centre for International Governance Innovation (CIGI), World Refugee Council Research Paper 12, 2019.

[2] M. Latonero, K. Hiatt, A. Napolitano, G. Clericetti, and M. Penagos, "Digital identity in the migration & refugee context: Italy case study," Data & Society, Tech. Rep., 2019.

[3] S. Madon and E. Schoemaker, "Digital identity as a platform for improving refugee management," *Information Systems Journal*, 2021.

[4] R. Read, B. Taithe, and R. Mac Ginty, "Data hubris? humanitarian information systems and the mirage of technology," *Third World Quarterly*, 2016.

[5] K. B. Sandvik, K. L. Jacobsen, and S. M. McDonald, "Do no harm: A taxonomy of the challenges of humanitarian experimentation," *International Review of the Red Cross*, 2017.

[6] E. Schoemaker, D. Baslan, B. Pon, and N. Dell, "Identity at the margins: data justice and refugee experiences with digital identity systems in lebanon, jordan, and uganda," *Information Technology for Development*, 2020.

[7] D. T. Abraha, "Blockchain-based solution for addressing refugee management in the global south: transparent and accessible resource sharing in humanitarian organizations," *Frontiers in Human Dynamics*, 2025.

[8] V. Vizgirda, R. Zhao, and N. Goel, "Socialgenpod: Privacy-friendly generative ai social web applications with decentralised personal data stores," in *Companion Proceedings of the ACM Web Conference 2024 (WWW '24 Companion)*, 2024.

[9] C. Esposito, R. Horne, L. Robaldo, B. Buelens, and E. Goesaert, "Assessing the solid protocol in relation to security and privacy obligations," *Information*, 2023.

[10] O. Gonzalez Benson, "Community mapping with resettled refugees: Reflections on embeddedness," *Collaborations: A Journal of Community-Based Research and Practice*, 2020.

[11] S. R. Caroll, I. Garba *et al.*, "The care principles for indigenous data governance," *Data Science Journal*, 2020.

[12] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS Quarterly*, 2003.

[13] E. M. Rogers, "Diffusion of innovations," *The Free Press*, 2003.

[14] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Quarterly*, 2004.

[15] K. Dorst, "The core of 'design thinking' and its application," *Design Studies*, 2011.

[16] T. Berners-Lee *et al.*, "Solid: A platform for decentralized social applications based on linked data," *MIT CSAIL*, 2016.

[17] Solid Project, "Web access control," https://solidproject.org/TR/wac, 2021.

[18] Solid Porject, "Access control policy (acp)," https://solid.github.io/authorization-panel/acp-specification/, 2022.

[19] M. D. Wilkinson *et al.*, "The fair guiding principles for scientific data management and stewardship," *Nature Publishing Group*, 2016.

[20] B. Mons, C. Neylon, J. Velterop, M. Dumontier, L. O. B. da Silva Santos, and M. D. Wilkinson, "Cloudy, increasingly fair; revisiting the fair data guiding principles for the european open science cloud," *Information Services & Use*, 2017.

[21] M. van Reisen, S. Y. Amare, R. Nalgula *et al.*, "Federated fair principles: Ownership, localisation and regulatory compliance (olr)," *FAIR Connect*, 2023.

[22] T. Berners-Lee, J. Hendler, and O. Lassila, "The semantic web," *Scientific American*, 2001.

[23] T. Health and C. Bizer, "Linked data: Evolving the web into a global data space," *Morgan & Claypool*, 2011.

[24] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly*, 1989.

Appendix A

List of Interviews & Participants

Table A.1 summarises the empirical material used for the needs analysis in Chapter 5 and subsequent analysis chapters. All participants are referenced using anonymised identifiers to preserve confidentiality.

Table A.1: Overview of interviews conducted

Code	**Stakeholder Type**	**Language / Mode**	**Notes**
NGO-A (Makeda)	NGO representative	English	Transcript split into two parts
NGO-B (Danial)	NGO representative	English	Single interview
Ref-A	Refugee participant	English (no translator)	Transcript available
R1	Refugee participant	Via translator (Tigrinya → English)	Transcript available
R2	Refugee participant	Via translator (Tigrinya → English)	Transcript available
R3	Refugee participant	Via translator (Tigrinya → English)	Transcript available
R4	Refugee participant	Via translator (Tigrinya → English)	No transcript available

Appendix B

Interview Transcripts

This appendix document the interview material which forms the empirical basis of the need analysis discussed in chapter 5 & the adoption analysis in chapter 8.

Due to the length of the interview material, the full interview transcripts are provided as separate files via an external repository.

All transcript files are available at the following google drive link:

- Interview Transcripts Repository

To protect confidentiality, all refugee participants are referred using anonymized identifiers. NGO representatives are referenced using their first names along with the identifiers.

The transcript set includes:

- NGO-A (Makeda), interview transcript (2 parts)
- NGO-B (Danial), interview transcript
- Ref-A, refugee interview transcript
- R1, R2 & R3, refugee interviews transcripts, conducted via a translator

One refugee interview (R4) was also conducted via a translator but could not be transcribed.

Appendix C

Coding & Analysis Trail

This appendix document the analytical process used to derive insights from the interviews conducted. It provides transparency regarding how raw interview material was coded, compared & synthesized into themes.

The coding process followed a qualitative analysis approach. The codes were grouped into thematic categories via comparison across participants & stakeholder groups.

The following raw analysis artefacts are provided as separate spreadsheet files:

- A coding labelling spreadsheet documenting the codes assigned on the basis of the interviews across all participants.
- A convergence-divergence analysis spreadsheet summarizing areas of alignment & difference between refugees & bewteen NGO perspectives.

All coding & analysis material are available at the following google drive link:

- Coding & Analysis Repository

Appendix D

Prototype Implementation & Demonstration

This appendix provide access to the prototype artefacts developed as part of this research.

The full source code for the prototype application is available via a Github repository:

- GitHub Repository

Due to file size limitation the recorded demonstration of the prototype application is provided via google drive:

- Prototype Demo Video

Appendix E

Collaboration

This appendix shows the collaborative development process of the emergency incident reporting prototype built in collaboration with FieldLab.

The overview of contributions & development process is available via:

- Collaboration Document