UNIVERSIDADE D
COIMBRA

Jorge Eduardo Rivadeneira Muñoz

A User-Centric Privacy-Preserving Model in the New Era of the Internet-of-Things

Tese no âmbito do Doutoramento em Engenharia Informática, Especialidade em Arquiteturas, Redes, e Cibersegurança, orientada pelo Professor Doutor Jorge Sá Silva, e pelo Professor Doutor Fernando Boavida, e apresentada ao Departamento de Engenharia Informática da Faculdade de Ciências e Tecnologia da Universidade de Coimbra.

Agosto de 2023

UNIVERSIDADE D
COIMBRA

Department of Informatics Engineering
Faculty of Sciences and Technology
University of Coimbra

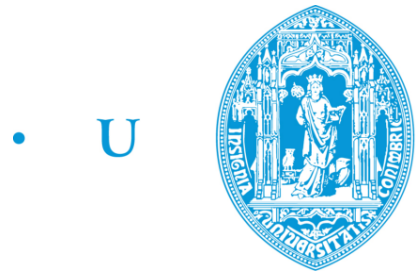
A User-Centric Privacy-Preserving Model in the New Era of the Internet of Things

Jorge Eduardo Rivadeneira Muñoz

PhD in Informatics Engineering
PhD Thesis submitted to the University of Coimbra

Advised by Prof. Dr. Jorge Sá Silva
and Prof. Dr. Fernando Boavida

August, 2023



Departamento de Engenharia Informática
Faculdade de Ciências e Tecnologia
Universidade de Coimbra

Um modelo de privacidade centrado no Utilizador para a Nova Era da Internet Das Coisas

Jorge Eduardo Rivadeneira Muñoz

Doutoramento em Engenharia Informática
Tese de Doutoramento apresentada à Universidade de Coimbra

Orientado pelo Prof. Dr. Jorge Sá Silva
e pela Prof. Dr. Fernando Boavida

Agosto, 2023

The research work presented in this thesis was supported by the Republic of Ecuador through SENESCYT – *Secretaría de Educación Superior, Ciencia, Tecnología e Innovación del Ecuador* under the PhD grant CZ02-000903-2018; by FCT – *Foundation for Science and Technology*, I.P./MCTES through national funds (PIDDAC), within the scope of CISUC R&D Unit - UIDB/00326/2020 or project code UIDP/00326/2020, and European Social Fund, through the Regional Operational Program Centro 2020.

"Details are all that matters: God dwells in these and you never get to see Him if you don't struggle to get them right"

Stephen Joy Gould

Acknowledgments

This doctoral thesis is the outcome of hard work, relentless dedication, and the generous collaboration of many people and organizations that have paved the way for the completion of this academic achievement. Therefore, the following words I am about to convey encapsulate a heartfelt thank you.

First and foremost, I would like to express my sincere gratitude to my supervisors, Professor Jorge Sá Silva and Professor Fernando Boavida. Thank you for giving me the invaluable opportunity to be part of your research group. Your unwavering support, guidance, patience, and commitment have played a crucial role in carrying out this work. Your guidance and deep knowledge have illuminated my path in this process. Without you, this accomplishment would have been impossible to achieve. Thank you once again for your immense impact on my academic and professional growth.

Likewise, I wish to extend my appreciation to the Centre for Informatics and Systems of the University of Coimbra (CISUC), particularly the Laboratory of Communications and Telematics (LCT), for welcoming me and allowing me to conduct my research. At this point, I would like to express my heartfelt thanks to Professor André Rodrigues for the valuable discussions we have had related to the topics addressed in this thesis.

Throughout this journey, I have had the privilege of sharing with incredible people to whom I am thankful for all their support. To my former colleagues, Soraya, Oswaldo, Duarte, Ngombo, thank you for your advice and recommendations on how to face this challenge. To Rui, Sandra, Ricardo, and Matheus, thank you for the good times and for always being willing to collaborate and share your knowledge. To Oscar and Guilherme, apart from the good moments shared, I appreciate and value your perseverance, proactivity, and responsibility in the tasks we have shared. To Marcelo and Érica, who are more than just colleagues, I consider them my friends. I am thankful for all your help and I am indebted to you for always being there and making me feel at home when I needed it the most. I also want to express my gratitude to Adriana, Mauro, Esther, Alex, Karima, David, Ricardo, Rui, Joca, and all the colleagues from the research center who never fail to provide advice or words of support.

Similarly, my appreciation extends to my friends: Pancho, Arita, Vane, Gabo, Andrés, Telmo, and Julio. Despite occasional distances, your consistent support and strong encouragement have been instrumental in propelling me forward.

This achievement would have remained unattainable without the support of my family. Hence, I extend my thanks and dedicate this effort to my parents, Jeannett and Marco, whose unending love and constant encouragement have been

my driving force throughout this journey. To my dear sister, Anita María, and my grandmother, Lelia, whose presence and affection have consistently provided strength and motivation at every step along the way.

Lastly, finding the precise words to express the profound gratitude I hold for my wife, María Belén, is not an easy task. For this reason, I dedicate this work to you. As you read these lines, I hope you remember that your love and consistent support have enabled us to accomplish this project which seemed so distant and unattainable five years ago. María Belén, I wholeheartedly thank you for every shared moment, for your dedication to our home, and for being my partner in this challenging yet wondrous journey. May God grant us health and life to continue pursuing dreams together. Your presence has been my wellspring of strength and inspiration, and this accomplishment is imprinted with the love and support you have continuously offered. My gratitude to you transcends words.

Abstract

Over time, the concept and the scope of the Internet of Things have evolved, and nowadays it is being boosted with new approaches where various elements are integrated into smart ecosystems. This goes beyond the mere interconnection of perception layer devices, giving rise to the notion of the Internet of Everything. On the road toward the latter concept, innovative Internet-of-Things-based paradigms propose the integration of human factors and activities as intrinsic elements within a hyperconnected world. Currently, Human-Centered Internet-of-Things leverages the widespread use of smart devices, their sensing capabilities, and their technical features, along with their seamlessly interactive nature, to carry out data acquisition and service provisioning. Systems based on these premises may be deployed within different domains, offering a wide variety of services.

While the benefits that Human-Centric Internet of Things systems offer to end users appear promising, there are still significant challenges to address, namely privacy and data protection. Currently, different regulations across the globe lay the legal groundwork to tackle these specific issues. These regulations demand the adoption of transparent practices for the collection, processing, and use of personal data, as well as more meaningful user involvement in privacy protection. In addition to the protective measures outlined by legal frameworks, an increasing number of people agree with the notion that data control mechanisms should be integrated into modern information systems. This empowerment of end users with the ability to manage their privacy settings is seen as essential, as relying solely on the safeguards of a legal framework, while exceedingly important, may not prove entirely effective. Moreover, despite the existence of user-centric solutions in the literature, there are no proposals that directly fall within the context of Human-in-the-Loop Cyber-Physical Systems.

Therefore, in this thesis, we delve into this specific context and address the challenge of privacy preservation from a user-centric approach. As a starting point, we review, analyze, classify, and discuss state-of-the-art contributions in the field of user-centric privacy preservation. We then present our privacy-preserving model, which results from the combination of two approaches: the first one is oriented toward the data acquisition phase, while the second approach is related to the state-inference phase. Additionally, we propose an integration model that aims to evaluate our model and foster the vision of smart and sustainable cities. Moreover, this thesis provides the details of our case studies, describes the development and implementation aspects of the components of each of our models, their assessment, and the respective results.

Keywords: Privacy Preservation, Internet of Things, User-Centric, Privacy Awareness, Human-in-the-Loop, Data Protection, Consent

Resumo

Ao longo do tempo, o conceito de Internet das Coisas e o seu alcance evoluíram e, hoje em dia, estão a ser impulsionados por novas abordagens, onde vários elementos são integrados em ecossistemas inteligentes. Isto vai para além da simples interconexão de dispositivos da camada de perceção, dando origem à ideia de Internet de Tudo. No caminho para este último conceito, paradigmas inovadores baseados em Internet das Coisas propõem a integração de fatores e atividades humanas como elementos intrínsecos num mundo hiperconectado. Atualmente, o Internet das Coisas centrada no Ser Humano aproveita o uso generalizado de dispositivos inteligentes, suas capacidades de deteção e suas características técnicas, juntamente com sua natureza interativa, para realizar a aquisição de dados e prestação de serviços. Sistemas baseados nestas premissas podem ser implantados em diferentes domínios, oferecendo uma ampla variedade de serviços.

Embora os benefícios que os sistemas centrados no Ser Humano da Internet das Coisas oferecem aos utilizadores finais sejam promissores, ainda existem desafios importantes a enfrentar, nomeadamente nas áreas da Privacidade e da Proteção de dados. Atualmente, diferentes regulamentos em todo o mundo fornecem a base legal para abordar estas questões temáticas específicas. Esses regulamentos exigem a adoção de práticas transparentes para a recolha, processamento e uso de dados pessoais, bem como uma maior participação do utilizador na proteção da sua privacidade. Complementarmente às medidas de proteção previstas nos quadros legais, cada vez mais pessoas concordam com a ideia de que os mecanismos de controlo de dados devem ser incluídos nos sistemas de informação modernos para capacitar os utilizadores finais com a capacidade de gerir as suas configurações de privacidade, uma vez que depender apenas da proteção de um quadro legal, embora extremamente importante, pode não ser eficaz. Além disso, apesar da existência de soluções centradas no utilizador na literatura, não existem propostas que se enquadrem diretamente no contexto de Sistemas Ciberfísicos com Humanos no *Loop*.

Assim sendo, nesta tese, exploramos este contexto específico e abordamos o desafio da preservação da privacidade a partir de uma abordagem centrada no utilizador. Como ponto de partida, analisamos, classificamos e discutimos contribuições de ponta no campo da preservação da privacidade centrada no utilizador. Em seguida, apresentamos o nosso modelo de preservação da privacidade, que é o resultado da combinação de duas abordagens: a primeira orientada para a fase de aquisição de dados, enquanto a segunda abordagem está relacionada com a fase de inferência do estado. Além disso, propomos um modelo de integração que visa avaliar a nossa solução e promover a visão de cidades inteligentes e sustentáveis. Além disso, esta tese fornece os detalhes dos nossos estudos de caso, descreve os aspetos de desenvolvimento e implementação dos componentes de cada um dos nossos modelos, a sua avaliação e os respetivos resultados.

Palavras-chave: Preservação da Privacidade, Internet das Coisas, Centrado no Utilizador, Consciência de Privacidade, Humano-no-*Loop*, Proteção de Dados, Consentimento

Foreword

The work detailed in this thesis was accomplished at the Laboratory of Communications and Telematics (LCT) of the Center for Informatics and Systems of the University of Coimbra (CISUC), in partnership with the Institute for Systems Engineering and Computers of Coimbra (INESCC), within the context of the following grants and project:

PhD grant - CZ02-000903-2018 financed by the Republic of Ecuador through Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT)

Research grant - IT137-23-010 under the CISUC R&D unit with reference UIDP/00326/2020 Center for Informatics and Systems of the University of Coimbra financed by the Foundation for Science and Technology (FCT), I.P./MCTES through national funds (PIDDAC)

PrivacyCoLab - Bilateral Initiative number 63 financed by EEA Grants Portugal 2014-2021. The goal of this initiative is to create a collaborative laboratory of researchers, students and professors between the University of Coimbra - Portugal and Østfold University College - Norway (OU) to propose, develop and evaluate an innovative model to respond to these new privacy requirements. Specifically, during one year of project life, it is intended to propose a new disruptive paradigm for smartphone devices. This project aims to address several issues, such as application monitoring, retrieval of (and information about) privacy policies, consent management, among other aspects. It is also intended to apply and evaluate the model created in a real-world environment.

MyPrivacy: More Data is More Privacy - Funded by INESC Coimbra, under the internal competition for scientific and technological research projects, specifically focusing on exploratory initiatives aimed at developing new areas or continuing ongoing research.

The outcome of the design, experiments, and assessments of several mechanisms on the course of this thesis resulted in the following publications:

Journal papers:

- Rivadeneira, J. E., Sánchez, O. T., Dias, M., Rodrigues, A., Boavida, F., and Silva, J. S. (2023d). Confluence: An integration model for human-in-the-loop iot privacy-preserving solutions towards sustainability in a smart city. *Submitted to IEEE Internet of Things Journal* **(Q1)**;
- Rivadeneira, J. E., Borges, G. A., Rodrigues, A., Boavida, F., and Silva, J. S. (2023a). A unified privacy preserving model with ai at the edge for human-in-the-loop cyber-physical systems. *Submitted to Internet of Things; Engineering Cyber Physical Human Systems* **(Q1)**;

- Rivadeneira, J. E., Silva, J. S., Colomo-Palacios, R., Rodrigues, A., and Boavida, F. (2023c). User-centric privacy preserving models for a new era of the internet of things. *Journal of Network and Computer Applications*, page 103695 **(Q1)**;
- Sanchez, O. T., Fernandes, J. M., Rodrigues, A., Silva, J. S., Boavida, F., Rivadeneira, J. E., de Lemos, A. V., and Raposo, D. (2022). Green bear - a lorawan-based human-in-the-loop case-study for sustainable cities. *Pervasive and Mobile Computing*, 87:101701 **(Q1)**; and
- Jiménez, M. B., Fernández, D., Rivadeneira, J. E., Bellido, L., and Cárdenas, A. (2021). A survey of the main security issues and solutions for the sdn architecture. *IEEE Access*, 9:122016–122038 **(Q1)**;

Conference papers:

- Rivadeneira, J. E., Jiménez, M. B., Marculescu, R., Rodrigues, A., Boavida, F., and Sá Silva, J. (2023b). A blockchain-based privacy-preserving model for consent and transparency in human-centered internet of things. In *Proceedings of the 8th ACM/IEEE Conference on Internet of Things Design and Implementation*, IoTDI '23, page 301–314, New York, NY, USA. Association for Computing Machinery;
- Rivadeneira, J. E., Sá Silva, J., Colomo-Palacios, R., Rodrigues, A., Fernandes, J. M., and Boavida, F. (2021). A privacy-aware framework integration into a human-in-the-loop iot system. In *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 1–6;
- Rivadeneira, J. E., Filipe Pinto, M., and Sá Silva, J. (2020). A qualitative study on trust perception in iot mobile applications. In *2020 IEEE Colombian Conference on Communications and Computing (COLCOM)*, pages 1–6;
- Torres, O., Dávila, G., Rivadeneira, J. E., and Hidalgo, P. (2020). A vulnerability analysis of the ieee 802.15.6 display authenticated association protocol. In *2020 IEEE Colombian Conference on Communications and Computing (COLCOM)*, pages 1–6;

Co-advisor of MSc Thesis:

- Rodrigues, J. (2022). *Novos Modelos de Privacidade para a Internet das Coisas*. Msc thesis, University of Coimbra, DEEC.

In parallel with the execution of the tasks related to this thesis, participation in different projects during this PhD course led to discussions and exchange of ideas that resulted in some publications listed above, which are framed within the context of this research and enriched the performed work. The cooperation underlying these papers encompassed several aspects, namely, the discussion and conception of ideas, the design and implementation of the experiments, and the analysis of data and results.

Contents

List of Figures

List of Tables

Acronyms

AI Artificial Intelligence

AID-S Adaptive Inference Discovery Service

API Application Programming Interface

APK Android Application Package

ATU Audit and Transparency Unit

BCIPRE Blockchain-based Condition Invisible Proxy Re-encryption

BLE Bluetooth Low Energy

BN Blockchain Network

CISUC Center for Informatics and Systems of the University of Coimbra

CM Consent Manager

CPRE Conditional Proxy Re-Encryption

CP-ABE Ciphertext-Policy Attribute-Based Encryption

CPS Cyber-Physical System

DAM Data Acquisition Module

DC Data Controller

DDM Data Dispatcher Module

DIS Device Information Service

DL Deep Learning

DO Data Owner

DR Data Requester

DRSM Data Requests and Subscription Module

DS Data Subject

EU European Union

EIF4SCC European Interoperability Framework for Smart Cities and Communities

FL Federated Learning

GATT Generic Attribute Profile

GBAD Gradient Boosting Anomaly Detector

GDPR General Data Protection Regulation

GE Generic Enabler

gRPC Google Remote Procedure Call

GUI Graphical User Interface

HCI Human-Computer interaction

HiTL Human-in-the-Loop

HiTLCPS Human-in-the-Loop Cyber-Physical System

HIPAA Health Insurance Portability and Accountability Act

HLF Hyperledger Fabric

INESCC Institute for Systems Engineering and Computers of Coimbra

IID Independent and Identically Distributed

IoE Internet of Everything

IoHT Internet of Healthcare Things

IoP Internet of People

IoT Internet of Things

IoTA IoT Assistant

IrDA Infrared Data Association

IRR IoT Resource Registry

ISABELA IoT Student Advisor and BEst Lifestyle Analyzer

ISD IoT Services Diffusion

ISPR IoT Service Providers Repository

ISS IoT Service Store

JSON JavaScript Object Notation

KD Knowledge Distillation

LCT Laboratory of Communications and Telematics

LDPO Local Differential Privacy Obfuscation

LSTM Long Short-Term Memory

M2M Machine–to–Machine

ML Machine Learning

MLP Multi-Layer Perceptron

MQTT Message Queuing Telemetry Transport

MSP Membership Service Provider

NLP Natural language Processing

NoNN Networks of Neural Networks

OSN Online Social Networks

P2P Peer–to–Peer

P3P Platform for Privacy Preferences

PA Privacy Assistant

PACHA Privacy-Aware Component for a Human-in-the-Loop IoT Approach

PARA Privacy Augmented Reality Assistant

PATA Privacy-Aware Task Assignment Framework

pawS Privacy Awareness System

PDC Personal Data Custodian

PDM Personal Data Manager

PEALS Privacy and Energy-Aware Location Service

PEB Privacy Enforcement Bridge

PEP Policy Enforcement Point

PET Privacy Enhancing Technologies

PII Personally Identifiable Information

PLA Privacy Level Agreement

PMEC Privacy Manager system based on Edge Computing

PMI Privacy Manager Instances

PoC Proof-of-Concept

PP Privacy Proxy

PPA Personal Privacy Assistant

PPI PACHA Privacy Interagent

PPM Privacy Preserving Mechanisms

PPO PACHA Privacy Orchestrator

PPSF Privacy-Preserving and Secure Framework

QoS Quality of Service

RE Regulatory Entity

ReLU Rectified Linear Unit

RSSI Received Signal Strength Indicator

SC Smart Contract

SDK Software Development Kit

SIoT Social Internet of Things

SNR Signal-to-Noise Ratio

SP Service Proxy

SRAC Selective Ring-based Access Control

SSC Sustainable Smart Cities

TAPAS Trustworthy privacy-aware participatory sensing

TIPPERS Testbed for IoT-based Privacy Preserving Pervasive Spaces

TLS Transport Layer Security

TPS transactions per second

TTN The Things Network

UI User Interface

UN United Nations

URL Uniform Resource Locator

UUID Universally Unique identifier

UX User Experience

VM virtual machine

VU virtual user

WP29 Working Party 29

XACML eXtensible Access Control Markup Language

XML Extensible Markup Language

Chapter 1

Introduction

Contents

The dawn of a new era in the IoT has arrived, with a profound shift that places humans at the core of its development. Termed as Human-Centric IoT, this evolution embraces new concepts, wherein individuals are intricately connected with and integral to the operation of these systems. Amidst this transformative landscape, privacy emerges as a paramount challenge to confront. This chapter furnishes the background, and motivation for the current research, which is directed toward tackling the critical issue of privacy-preservation in this new era of the IoT. Moreover, the thesis objectives and contributions are expounded upon. Finally, an outline of the document's structure is provided, offering a clear roadmap for the reader.

1.1 Background and Motivation

Networking evolution has led us to a world of ubiquitous connections, from small devices to large components seamlessly interacting with each other, even without human intervention, in what we now know as the IoT. Based on this paradigm, the scientific community has been able to define and propose new mechanisms for obtaining, processing, and communicating real-time data from the environment, through the use of sensors, actuators and portable devices, with the aim of either improving the quality of life [Al-Fuqaha et al., 2015], or optimizing and automating industrial processes. According to Cisco's forecasts and trends [Barnett et al., 2018], Machine–to–Machine (M2M) communication has grown exponentially, from 6.1 billion connections in 2017 to almost 15 billion by the end of 2022, reaching a traffic of around 25 Exabytes. Moreover, this trend is leading to an even greater traffic rate increase due to multimedia applications in areas such as smart-car navigation and smart healthcare.

Naturally, the IoT scope is constantly evolving and nowadays it is being extended with approaches where other elements are integrated into these smart domains, beyond the mere interconnection of perception layer's devices [Al-Fuqaha et al., 2015]. Innovative IoT-based paradigms propose the integration of the end-user as an integral part of this hyperconnected realm [Boavida et al., 2016]. These particular paradigms include approaches namely People-Centric IoT, Social Internet of Things (SIoT), Internet of People (IoP), and Human-in-the-Loop (HiTL) control for Cyber-Physical Systems (CPSs) [Wood and Stankovic, 2008; Nunes et al., 2015].

Taking a human-centric approach, IoT-based systems extend the spectrum of services and solutions to a large variety of areas, and at the same time, they spawn many technological and multidisciplinary challenges. Naturally, a substantial part of these challenges relates to technological aspects such as the device, the network, or even the data. Among the most important are connectivity, mobility, ubiquity, high availability, fault tolerance, Quality of Service (QoS), interoperability, reliability, and security [Boavida et al., 2016]. However, one of the most relevant challenge in this kind of approach is privacy [Grace and

Surridge, 2017]. Especially in these new-generation IoT paradigms, where the personalization of a provided service is a function of the acquired data, the more data available, the more profile-oriented the outcome. As a result, more privacy is demanded.

Nevertheless, we must recall that privacy is not only a technological challenge but a multidisciplinary one, since it includes human factors interacting with and within a digital environment. Each person has a different perception of how to deal with privacy, as there are users who have more concerns than others. A clear example is the way we handle conventional devices such as smartphones, where applications require different permissions to access files or execute actions. In this case each of us will have different concessions that meet our needs.

In 2018, General Data Protection Regulation (GDPR) came into force, stating fundamental rights for European Union (EU) citizens concerning the use of their personal data [Edwards, 2016]. This regulation contemplates two prime actors: the Data Subject (DS) and the Data Controller (DC). The former is identified or identifiable natural persons from whom the data is collected. The latter is the entity that "alone or jointly with others, determines the purpose and means of the processing of personal data" [Parliament et al., 2016].

As long as there is no legal bond by the DC, the GDPR states that the collection of personal information can only happen after notice and through the express consent of the DS [Cate, 2006]. Moreover, according to GDPR Art. 4-11, data processing consent must be freely given, by means of an affirmative, clear, informed, specific and unambiguous statement or action [Parliament et al., 2016]. This consent is no longer free when the DS has no possibility of refusing without suffering detriment.

To be better aligned with what is stipulated in the European Regulation, and to face the privacy challenge in mainstream IoT environments, many authors have contributed to the state-of-the-art with different proposals to assure users that their data is properly acquired, processed and stored. However, some of these contributions are leaving out or limiting the human interaction or participation in the decision-making process.

From the users' perspective, the simple act of being left apart from a system that is handling their data, could eventually affect its adoption [Munjin and Morin, 2011; Lafontaine et al., 2021], its trust perception and also raise some concerns such as: Where do the data go? For how long will the data be stored? With whom will the data be shared? What kind and how much information can be inferred from the collected data? How could this jeopardize user privacy? Are the privacy policies properly announced to the users? Can users control to some extent the information that they are sharing? These are the questions that research initiatives are trying to address by proposing user-centric privacy-preserving models. At this point it is important to emphasize that although there are already proposals in the state of the art aimed at granting a certain level of control to the user in this context, none of them focuses on the concept of Human-in-the-Loop Cyber-Physical System (HiTLCPS).

1.2 Objectives

The main objective of this research is to address the challenge of privacy preservation from a user-centric perspective in the context of HiTLCPSs, a concept that is framed within the set of proposals that encompass this new era of the IoT. To achieve this goal the following objectives have been established:

- Review and evaluate the state-of-the-art of existing contributions in the field of privacy preservation with a user-centric approach in the context of an evolved IoT paradigm.
- Identify, discuss, and summarize possible challenges and open issues in this field.
- Propose a new framework for privacy-preserving data acquisition in the realm of HiTLCPSs, that merges the best features from the existing contributions in the literature with innovative features.
- Design and develop a unified privacy-preserving model for HiTLCPSs based on the proposed framework.
- Design and develop a model that integrates different privacy-preserving HiTLCPSs to be applied in a realistic scenario (e.g., a smart city).
- Validate the new models by extending our current HiTLCPSs case studies. This task will comprise new implementations, deployment, and different assessments.

1.3 Contributions

Taking into consideration the goals described above, this thesis has produced the following contributions:

- **Review of the state-of-the-art regarding user-centric privacy preserving models** In order to gain a comprehensive understanding of the current contributions in this field, and identify the gaps in the existing research we performed a literature review. This is covered in Chapter 2.
- **Creation of classification for user-centric privacy-preserving models** In the state-of-the art, proposals that revise and categorize user-centric privacy preserving models in this particular IoT context are scarce. In order to set a common language for the analysis we created a classification. This is covered in Chapter 2.
- **Creation of a new privacy-preserving model for HiTLCPSs** After studying the concept of HiTLCPSs, we proposed two privacy-preserving approaches oriented to the data acquisition and state inference phase respectively. Based on these two approaches a new privacy-preserving model for HiTLCPSs is created. This is covered in Chapter 3.
- **Definition of a new framework for HiTLCPSs** From the reviewed models in the state-of-the-art, we extracted certain features that were

later used to build and define our framework. This framework was then employed in the development of our initial approach, which encompasses the privacy-preserving model. This is covered in Chapter 3.

- **Creation of a new decentralized consent management procedure for HiTLCPSs** One component that integrates the data acquisition phase of our privacy model is consent management. In this regard, one of our contributions is the development of a decentralized consent management process to enhance transparency. This is covered in Chapter 3.
- **Creation of a new model for integrating privacy-preserving HiTLCPSs** After proposing the privacy preservation model, the subsequent step involved creating a solution that enables the integration of various privacy-preserving HiTLCPSs to address a specific requirement. In our case, our model is oriented toward promoting sustainability in smart cities. This is covered in Chapter 4.
- **Development of a new HiTLCPS case study** Alongside the implementation of the privacy model, we also developed a new case study proposal focused on the sustainability of smart cities. This is covered in Chapter 5.
- **Creation of a new platform that integrates different services from HiTLCPSs** Each case study came with its own dedicated platform, despite sharing certain features. Capitalizing on this, we developed a new platform that facilitates the integration of services offered by the individual platforms. This is covered in Chapter 5.
- **Creation of a Federated Learning model for state inference in HiTLCPSs** In our HiTLCPSs case studies, the inference process has traditionally been conducted using machine learning models on servers outside the user's control (e.g., servers in a cloud managed by the inference process responsible). To establish an inference process that does not require data to leave the user's device, we employed Federated Learning and developed a new model. This is covered in Chapter 6.

In addition to the aforementioned contributions, it is important to highlight the dissemination of our work throughout the global scientific community, accomplished through publications in international journals and conferences. The succeeding sections of this document will now delve into the underlying foundations that substantiate these contributions. Following this, the subsequent section outlines the structure and content of the rest of this document.

1.4 Outline of the Thesis

Apart from the introduction, this thesis is structured into six additional chapters.

Chapter 2 commences by giving an overview of the evolution of the traditional IoT concept toward novel paradigms where end-users and their data play

a crucial role. Privacy stands out as a major challenge in these paradigms. Subsequently, a thorough review and analysis of current user-centric privacy-preserving models follow, wherein they are categorized based on a proposed classification. Finally, challenges and open issues are identified and discussed.

Chapter 3 introduces the concept of HiTLCPSs and its distinct phases. Following this, it presents two approaches to privacy preservation: one focused on the data acquisition phase and another aimed at the state inference phase. These two approaches pave the way toward a unified privacy-preserving model for HiTLCPSs.

Chapter 4 proposes a new model that serves as a reference for the development, implementation, and integration of innovative privacy-preserving HiTLCPSs. This model not only addresses the immediate requirements of our specific context but also holds the potential for broader applications across various domains. While its adaptability makes it suitable for diverse settings, our primary focus lies in leveraging this integration model to significantly enhance urban sustainability. By promoting seamless interoperability among the technological components of stakeholders within a smart city, our objective is to drive positive ecological and social outcomes.

Chapter 5 delves into two case studies exemplifying the implementation of the HiTLCPS concept. Each of these case studies revolves around the deployment of distinct platforms, individually tailored to address different objectives in specific contexts. Subsequently, the chapter introduces SPACES, an implementation solution aiming to combine simultaneously different contexts and integrate the services offered by the aforementioned platforms while considering the components of the models proposed in Chapters 3 and 4. This chapter provides technical details regarding the development of these components and their underlying technology.

Chapter 6 addresses the assessments of the models and their results. The first two sections of this chapter approach the evaluations from a quantitative perspective. Additionally, this chapter includes a section dedicated to a qualitative study conducted to understand the perception of trust in IoT mobile applications, a relevant aspect shared by the platforms derived from the case studies described in the previous chapter, as well as the current platform.

Chapter 7 concludes the document, offering a synthesis of the thesis, a compilation of the resulting contributions, and an identification of possible research paths for continuing the work presented in this thesis.

Chapter 2

A Review of User-Centric Privacy Preserving Models in a New IoT Era

Contents

Concepts emerging from the IoT propose the integration of the human factor as a fundamental component within interconnected ecosystems, enabling the provision of novel services and features. However, the data acquisition process conducted by devices facilitating the deployment of these new paradigms raises concerns regarding the type of information these entities can collect and infer. In many cases, users remain unaware that their information is being gathered and lack necessary control over these data flows. Currently, data protection regulations advocate for the adoption of transparent practices that encompass adequate notification mechanisms, effective consent management schemes, and the development of models that empower users as active participants with complete control over data flows, incorporating privacy preservation techniques.

In this chapter, we begin by providing an overview of the evolution of the mainstream IoT concept toward new paradigms where end-users and their data play a key role. One of the main challenges in these paradigms is privacy. We then conduct a revision and analysis of current user-centric privacy-preserving models, categorizing them based on a proposed classification. Finally, we identify and discuss challenges and open issues that can serve as starting points for upcoming research initiatives in this domain.

2.1 A new IoT Generation and Privacy Preservation

Typically, technology is created and developed with the objective of supporting humans in their tasks, from simpler to more convoluted activities, becoming a powerful ally over time. In this vein, traditional analogue models have been reshaped into cyber-physical environments comprising a variety of interconnected devices to support human activities by as many services as we can imagine, giving rise to what is commonly known as IoT. In this process, the relation between humans and IoT-based systems has become a focal point, giving rise to all sorts of privacy concerns.

2.1.1 Toward a new IoT Era

The IoT paradigm is built upon the idea of seamless integration, grouping, interconnection, and interaction of heterogeneous objects and devices in communication networks [Gubbi et al., 2013; Al-Fuqaha et al., 2015]. Realizing this vision is not straightforward due to the various challenges that need to be addressed [Koohang et al., 2022], including availability, reliability, security, management, scalability, and privacy. Before the emergence of the IoT paradigm, the Ubiquitous Computing notion already explored the idea of a closer and more natural relationship between users and computing devices.

This paradigm is in a constant ever-changing toward what is already known as Internet of Everything (IoE) [Langley et al., 2021; Miraz et al., 2015]. The

evolutionary process has giving rise to new concepts where the human factor is an essential component within an overall technological ecosystem. In the literature, there is a vast number of approaches that leverage this vision, including, among others: People-Centric IoT [Silva et al., 2017], HiTLCPSs and Internet of All [Nunes et al., 2015], Crowdsensing [Shu et al., 2017; Lashkari et al., 2019], Social Sensing [Wang et al., 2019a], SIoT [Rho and Chen, 2018], and IoP [Guillén et al., 2014; Boavida et al., 2016]. There are even approaches where humans are modeled as sensors within a system [Wang et al., 2014], leveraging the fact that, typically, users carry one or more smart devices with multiple, active, and built-in sensors of different nature and characteristics composing walking sensor networks.

Another possible way where humans contribute to an IoT environment in order to achieve a social objective or make the relevance of an event of interest known to a specific group of people, is through Crowdsensing [Shu et al., 2017]. For this data acquisition technique, the members of a community collect information using their own smart devices such as smartphones, smartwatches, and even from their social networks, in what is known as a Social Sensing.

An alternative way of interaction between IoT and Online Social Networks (OSN) is what is known as SIoT [Atzori et al., 2012]. This paradigm explores the assumption that objects or "things", within IoT, are capable of autonomously establishing social relationships with other objects. Similarly, the concept supports the idea of an ecosystem where people and smart objects can interact within a social structure of relationships. SIoT is positioning itself to become one of the most popular applications paradigm [Rho and Chen, 2018].

Regarding IoP, Boavida et al. [2016] argue that it can be considered as a specific area within the IoT paradigm, where the source and sink of data are the humans and their interactions, while in Miranda et al. [2015] this concept is seen as closing the gap between humans and the IoT, thus achieving total integration and paving the way for the development of new services and applications.

Currently, these IoT-based variants and its applications play an essential role in providing better quality of life for people [Petrov et al., 2019]. Thus, the development of platforms, systems, and applications based on this approach, able to obtain and process data through user interaction or by built-in sensors within the user's devices, is a topical issue.

Nevertheless, it must be recalled that the fuel for all the possible implementations of these concepts as a highly integrated technological environment with several services, ends up being the same. We refer as fuel as the data that user's appliances and interconnected devices can capture, such as physical conditions, environmental states, sensor variations, preferences, activities, location, social network's data, among others. Such data can be exploited and analyzed either by whoever captures them or by third parties and, in the case of misuse, this could eventually threaten and/or jeopardize the user's privacy.

2.1.2 Privacy-Preservation

Barhamgi et al. [2018] argue that existing solutions that are intended for privacy protection in CPSs do not meet the objective of implementing controls to notify the users about the purpose of information collection, when, by whom, and for what reason. There is a clear lack of transparency around these systems, which leads users to be unaware of the volume of sensitive information that can be collected, processed, shared and even worse, inferred [Lippi et al., 2019]. An average user is generally unaware of how securely their information is stored [Rao et al., 2016], or the amount of sensors that exist in their surroundings [Lee et al., 2018], or even which devices are currently collecting personal information, making them vulnerable to attacks, whether they consist of identity theft or scams [Rashtian et al., 2014]. All this adds up to the users' lack of knowledge about topics such as privacy policies and preferences [Smith, 2003]. Moreover, systems that gather personal information focus on extracting and processing as much data as possible to maximize their revenue, rather than considering user privacy, and merely state data usage policies and user guides, forgetting the integration of privacy mechanisms within their models. Last but not least, given the undeniable relationship between data security and privacy, privacy in the context of devices is often limited to mechanisms that target the security of the hoarded data [Corcoran, 2016].

All this adds up the dichotomy presented by Pötzsch [2009], in which it is mentioned that although there are people who are generally aware of privacy (stated attitude), their actions could be contradictory(behavior). This is known as the Privacy Paradox. This author argues that one way to overcome this problem is not only with technical solutions, but also considering behavioral and cognitive aspects. The author concludes that people can only make informed decisions when, in addition to knowing the possible benefits of disclosing personal data, they are informed about privacy risks and the possible intentions of data recipients, in other words, the potential privacy hazards.

In this sense, it can be argued that although technology has taken giant steps toward an information-driven world, humans are losing prominence within this ecosystem, and privacy is being threatened for the sake of information value. In addition, we must not neglect that privacy is an inherent human right that spans both the physical (offline) world and the digital (online) world. In fact, according to the United Nations (UN), human beings have the same rights, whether they are in a digital environment or in a real environment [Chander and Land, 2014; Nyst and Falchetta, 2017]. To safeguard privacy within the digital side, this organization has requested all countries to review the methods, practices, and legislation regarding the surveillance and interception of communications. In this respect, EU-GDPR seeks to align with the UN requirement, although, as mentioned by Notario et al. [2014], having a consistent legal framework is not the ultimate solution, since this does not guarantee that stakeholders adopt practices regarding privacy. Moreover, it is crucial to provide users with platforms, systems and transparent mechanisms that allow them to effectively re-gain control over their information [Edwards, 2016].

Currently, DCs are using different mechanisms for data acquisition, which can undermine the privacy of the DS. It is for this reason that the current proposals for the control and preservation of privacy by the user are through intermediary systems or entities. Intermediary components are modules typically positioned between the DS and DC, more specifically within the data distribution pipeline. Roughly, these intermediaries may contain one or more mechanisms that support and/or provide user's privacy preservation. A closely related concept is proposed by Davies et al. [2016], where these intermediaries are called privacy mediators. According to the authors, these mediators allow the DS, among other things, to control the release of their data.

2.2 User-Centric Privacy Preserving Models

During the last decade, the state-of-the-art has considerably grown, with a fair number of privacy-preserving approaches in various areas and some proposals for their classification. For example, Vergara-Laurens et al. [2017] classify Privacy Preserving Mechanisms (PPM) for Crowdsensing, while in Satybaldy and Nowostawski [2020] a taxonomy of privacy preservation techniques based on blockchain is elaborated.

In health cloud environment, Kanwal et al. [2021] propose a classification of requirements for privacy preservation solutions and more closely related to the IoT sphere, there has been some taxonomic efforts. For instance, Firoozjaei et al. [2020] propose a taxonomy for privacy-preserving solutions for blockchain-based IoT applications, while the categorization made by Kounoudes and Kapitsaki [2020] is based on GDPR features and challenges.

Our review is structured according the classification proposed in Figure 2.1 and aims to provide an order to the contributions that come under the realm of user-centric privacy-preserving models. This sort of proposals pose end-users a way to empower themselves with the control of their privacy aspects, and their interaction is essential. For instance, a DS can discover and select IoT resources in his/her vicinity, set privacy preferences manually or through assistance, grant and revoke consent, etc. In this chapter we will focus mainly on this subset of privacy-preserving solutions since we consider that in the new generation of the IoT, the role of the human should not be limited only as a data source but an active element able to interact and coexist within this ecosystem, accessing services or be part of them without their rights being affected. Which is consistent with the idea set forth by Nunes et al. [2015], that *"human technology is made by humans, for humans"*.

The proposed classification consists of four categories. The first group of models is organized based on what has been labeled as the smart domain. This category encompasses four areas: Smart Cities, Smart Buildings, Smart Homes, and Smartphones. Each of these areas incorporates various technologies aimed at enhancing users' quality of life and their experiences. However, they all share a common characteristic: their operations are primarily data-driven. While this feature is essential, it also gives rise to privacy concerns.

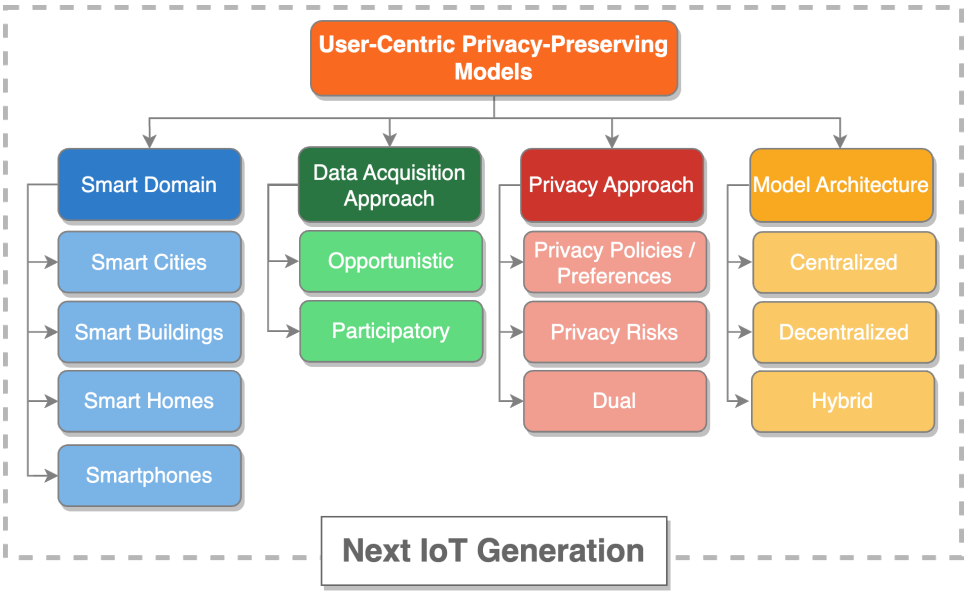


Figure 2.1: Proposed classification for User-Centric Privacy Preserving Models

The second category organizes the contributions based on the approach to data acquisition. Data can be collected either opportunistically or through participatory means. Opportunistic sensing is a passive form of data collection that occurs with minimal direct user interaction with applications, sensors, or personal devices [Guo et al., 2013], and sometimes without any interaction at all. Conversely, participatory sensing involves users actively participating in the data collection process by completing assigned tasks such as taking a photo or sharing specific data in a particular moment or venue [Pournajaf et al., 2016].

The third division classifies models based on their privacy approach, categorizing them into three subsets: Privacy Policies and Preferences, Privacy Risks Estimation, or a Dual Approach. The first subset includes models that require the definition of privacy policies and their incorporation into a decision-making phase. The second category encompasses proposals that rely on privacy risks as their underlying mechanism. In other words, these models include a dedicated component within their structure responsible for assessing the risks associated with the information intended to be disclosed to a DC. The last category consists of methods that implement a combination of both approaches, incorporating elements from both Privacy Policies and Preferences as well as Privacy Risks estimation.

Lastly, the fourth group classifies models based on their architecture. Historically, centralized models have been prominent in the state-of-the-art. However, in recent years, new alternatives have emerged, promoting decentralized approaches or even hybrid models. In the case of hybrid models, certain tasks or processes require an intermediary entity to execute them, while for other functions, the mediator becomes dispensable.

2.2.1 Smart Domain

The integration of places, services, and devices, used by citizens to carry out their daily activities, is increasingly seamless, transforming the environment around them into an intelligent ecosystem. At present, each of the components that comprise a smart domain is studied and approached individually due to their intrinsic characteristics. However, a common concern that rise all the areas that comprise an smart domain is privacy preservation. Within the literature there are some proposals that aim to mitigate this issue [Seliem et al., 2018]. For instance, Eckhoff and Wagner [2018] review building blocks for Privacy Enhancing Technologies (PET) within a smart city context. Based on their analysis, they were able to propose a set of strategies at the system design level, to incorporate privacy aspects. Similarly, a taxonomy is proposed to classify risks, comprising five types of privacy, namely privacy of location, privacy of state of body and mind, privacy of behavior and action, privacy of social life, and privacy of media.

An alternative that aims to ensure security and privacy for data dissemination in a smart-city context is SMARTIE, a people-centric IoT platform proposed by Martínez et al. [2017]. This approach is intended to provide end-users with a flexible and scalable model to protect the access to smart meters data. To address privacy requirements, SMARTIE's architecture includes a policy-based authorization model along with advance cryptographic scheme. Under such approach, SMARTIE's users are empowered to define their own access control preferences through eXtensible Access Control Markup Language (XACML), integrating Ciphertext-Policy Attribute-Based Encryption (CP-ABE). The authors of this proposal consider that the next step for this framework is a deployment on FIWARE, one of the main reference IoT platforms [Sinche et al., 2020b].

In order to guarantee the security and privacy of data and communications within IoT applications like smart homes, smart cities, smart grids, and healthcare, Banerjee et al. [2019] introduce a lightweight anonymous user authenticated session key agreement scheme. This scheme emphasizes anonymity and untraceability as its core features. It employs a three-factor authentication method that utilizes smart cards, passwords, and biometric information of the DS to establish secure communication. Furthermore, Kumar et al. [2019] propose another authentication-based approach specifically designed for smart grids, aiming to ensure data integrity, anonymity and untraceability.

In the study conducted by Makhdoom et al. [2020], the authors introduce "PrivySharing", an innovative framework supported by blockchain technology that aims to facilitate secure and privacy-preserving sharing of IoT data within a smart city environment. The key novelty of this work lies in the design of blockchain channels, which are divided into specific categories such as health, mobility, energy, and finance, allowing a limited number of organizations to process data within each channel. This division ensures focused data processing in accordance with the context of smart cities. Moreover, the framework employs smart contracts to regulate and embed an access control process, enabling organizations to access user data while ensuring compliance with the GDPR. However,

the authors acknowledge the need for a secure integration system to connect IoT devices with the blockchain network, which is an aspect that requires further attention and implementation.

Pappachan et al. [2017] propose a privacy-aware model for smart-building environments, which is made up of three main components. The first component is the IoT Resource Registry (IRR), responsible for broadcasting the data collection and sharing policies of IoT technologies that are going to interact with the DS. The second component, dubbed IoT Assistant (IoTA), manages user notifications regarding the privacy policies issued by IRRs, and allows the set-up of privacy preferences. The last element is the Privacy-Aware smart building management system, based on the Testbed for IoT-based Privacy Preserving Pervasive Spaces (TIPPERS) [Mehrotra et al., 2016]. The latter component has the function of receiving user privacy preferences and enforcing what is stipulated by the user when an IoT device begins to capture the data. As a first point, through TIPPERS, the building administrator defines the data collection and management policies within the smart location, which will be distributed by one or more IRRs. Once the policies have been established, the sensors begin the data gathering process. By the time the user accesses the premise, the IoTA installed on the user's handheld device will be able to discover the IoT devices around it, along with their privacy policies. The IoTA displays the relevant elements of these policies to the user, based on the privacy preferences. The relevance that IoTA gives to an element of the policy is based on a modeling of the user's privacy preferences learned over time. Figure 2.2 illustrates the interactions between each of the elements of this framework. In this model, privacy policies and preferences have been defined using a language based on JavaScript Object Notation (JSON)-Schema v4.

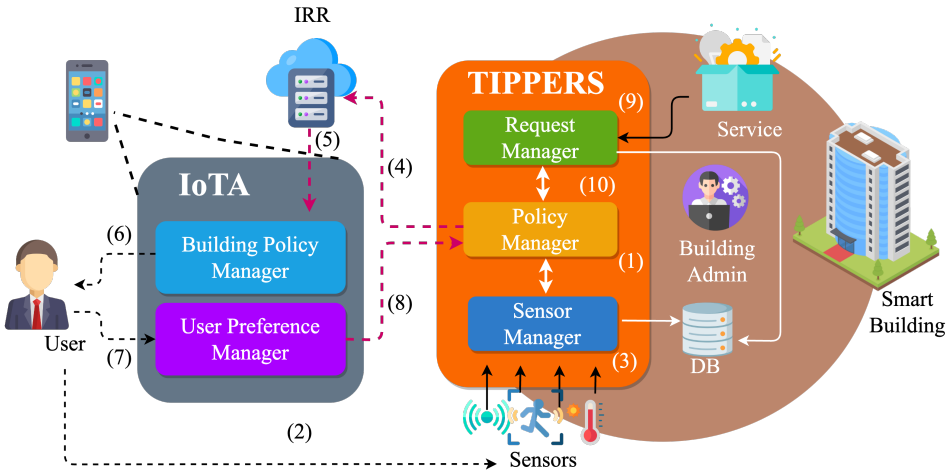


Figure 2.2: Testbed for IoT-based Privacy Preserving Pervasive Spaces. Adapted from Pappachan et al. [2017]

In a smart-home context, Chhetri and Genaro Motti [2022b] first conducted a qualitative study and based on their findings propose a privacy control framework with the aim of guide designers. The framework highlights several factors associated to privacy controls such as data-related controls, transparency, cent-

ralized interface, device control, multi-user controls, user support and security controls. An implementation of this framework in a prototype fashion called MyCam is carried out in Chhetri and Genaro Motti [2022a].

Zavalyshyn et al. [2018] propose HomePad, a privacy-aware smart hub for smart-homes. The goals of this model are empowering end users with a way to control which applications can access and process sensitive data collected by smart devices, and limit applications' execution unless they fulfill the privacy restriction set by the DS. HomePad manages the access to all smart home devices and provides a platform for applications execution. The DS can access the hub through a management interface to install and uninstall home apps, register new smart devices, and set privacy policies. HomePad exposes an Application Programming Interface (API) through which home apps can obtain sensed data, send data to actuators, access Internet services and perform data computation. For the implementation, the authors developed four applications, namely Lights Control, FaceDoor, Tide Pooler, and Spotify Control. According to the performance assessment, HomePad introduces an overhead between 4.7% and 6%, and the execution time varies between 2.2 and 4.1 seconds. The authors claim that these overheads do not hamper the User Experience (UX).

To enhance privacy awareness concerning the data gathered by IoT devices in smart homes, a solution called PrivacyCube has been proposed by Muhander et al. [2022]. PrivacyCube serves as an interactive device that enables DS to acquire knowledge about the IoT devices present in their surroundings and their respective data practices.

According to Wijesundara [2020], some privacy violations occur when smart homes' occupants interact with shared smart devices through User Interface (UI). Thus, an adaptive UI framework is proposed to model different user privacy preferences, user capabilities, and UI preferences. This proposal includes algorithms for detecting privacy violations and adapt the UI to fulfill users' privacy preferences without hindering usability. In contrast to other models, these privacy preferences are represented with the Rei policy language [Kagal et al., 2003]. To overcome the lack of users' control over their privacy in smart homes, a privacy decision model is proposed by Keshavarz and Anwar [2018]. This proposal seeks to assist users to easily express their privacy preferences. To carry out this task, the model leverages ML techniques to classify information as sensitive or non-sensitive.

A smart-home data inference framework based on ML models is proposed and implemented by Kounoudes et al. [2021] as a privacy tool called PrivacyEnhACT. The idea behind this proposal is to notify the user regarding unwanted inferences that could happen after processing different types of environmental data such as temperature, humidity, sound level, light intensity, motion a real time water flow consumption. These notifications are meant to be used as a privacy awareness mechanism to aid DS to refine the privacy setting of the collecting devices. This model could be complemented with EPIC, a privacy-preserving traffic obfuscation framework that prevents traffic analysis attacks [Liu et al., 2018] within an smart home environment. Its core is a utility-optimal differential privacy

mechanism to obfuscate the traffic flows' source, and also a privacy-preserving multihop routing model to assure unlinkability between source and destination. Another approach, described in Datta et al. [2018], involves shaping traffic flows. In this case, the authors propose, develop, and evaluate a Python library that enables the fitting of traffic to fixed distributions, effectively obfuscating user activity.

Xu et al. [2018] introduce a framework called Local Differential Privacy Obfuscation (LDPO) for data analytics, aiming to preserve data privacy while maintaining data utility. The framework operates by distilling IoT data on edge servers, utilizing a two-layer privacy approach. The first layer focuses on minimizing data on the IoT device itself, while the second layer implements obfuscation on the intermediate edge server. Data aggregation plays a crucial role in this server to prevent information leaks and reduce communication overhead. Certain user contents are customized based on requests from a DS, while others are diffused. Implementing LDPO faces several challenges, including designing lightweight algorithms to support real-time services, developing practical schemes for verifying privacy computations on resource-constrained IoT devices, and finding a suitable balance between data privacy and data utility.

Closer to the user level, we find the smartphone, one of the most popular smart devices with greater adoption and use in society. In this kind of devices, privacy problems are considerable. Smartphones are immersed in our daily lives, and generally they are equipped with a wide variety of sensors, communication interfaces, and considerable processing power. Thus, they represent a potential privacy risk [Dai et al., 2017]. A large amount of private information can be inferred from the data that the built-in sensors can capture. To ease this, Xu and Zhu [2015] propose SemaDroid, a privacy-aware sensor management model, to provide fine-grained access control over the smartphone's sensors. This framework allows the user to check sensors' usage by a third-party app based on the context and on the quality of the sensor data being supplied. To define in what context the data acquisition is allowed and the level of quality for the sensor data, SemaDroid uses Extensible Markup Language (XML) sensor usage policy.

Another alternative to prevent privacy inference attacks based on Android sensors data is Sensor Guardian [Bai et al., 2017]. This privacy protection system comprises two approaches. The first is a static instrumentation technique to insert hooks into the code of an Android Application Package (APK) file and control API calls used for accessing sensors. The second one is a policy manager running on the Android device as an app, managing and deploying control policies for the instrumented application. These policies allow or deny access to the sensor's data. Liu et al. [2016] propose a Personal Privacy Assistant (PPA) for mobile app permissions, this PPA is able to identify a suitable privacy profile following the preferences established by the user. According to the privacy profile the PPA recommends to the DS a group of permission settings.

2.2.2 Data Acquisition Approach

Another possible classification for this kind of privacy-preserving models is based on the data acquisition approach. Boubiche et al. [2019] present a taxonomy based on scalability criteria, the sampling rate, and the user involvement level. However, for our classification, we define two scenarios, one based on opportunistic sensing, and other based on participatory sensing.

Wang et al. [2013] propose a framework to mitigate the privacy problems associated with the opportunistic sensing of groups of users' location, named Privacy and Energy-Aware Location Service (PEALS). PEALS privacy model is based on the collection of privacy and energy preferences, along with the position of all the members of the group, as well as the privacy policies, the level of precision regarding the location, and the energy requirements for the operation of a mobile application. PEALS acts as an intermediary or broker between users and mobile applications that require user location for their operation. The framework determines whether the position of a particular DS (consumer's location) can be replaced by the one from another member of the contributor group when it is delivered to a mobile application. In this sense, it safeguards the privacy of the consumer (based on a privacy preference) and achieves energy savings on the user's device since the sensor or sensors intended for geolocation are deactivated.

Lee et al. [2018] proposed and developed a system named IoT Service Store (ISS) (Figure 2.3), based on a client-server approach. This implementation allows users to discover and interact with IoT services, announcing the privacy implications of their use. Additionally, ISS allows DS to control the collection and use of information obtained through the sensors. IoT services are registered within ISS, including data collection policies, possible inferences that can be derived from the collected information, and the service evaluation in terms of benefits and privacy risks using a five-star rating system. Each IoT service broadcasts a Bluetooth beacon containing a unique Uniform Resource Locator (URL), which will be detected by the user's device. This URL redirects the user to a website hosted on ISS, which contains information regarding the IoT service and its privacy policies. Possible interactions between the user and ISS include the subscription to a particular IoT service, the privacy preferences set-up, and service rating, among others. In addition to the system implementation, the authors proposed an information architecture to correlate the data obtained by the sensors with the personal information that can be inferred from it, thus contributing to achieve a better understanding of privacy risks by users, whenever they agree to use a certain service. For this architecture, the authors defined eight data types that can be obtained by sensing, against sixteen types of personal information that can be inferred.

In the context of location-based services deployed through opportunistic sensing, there are some proposals and techniques for privacy preservation. Unfortunately, in scenarios where participatory sensing prevails, these techniques are not directly applicable, since the participant is required to provide additional information.

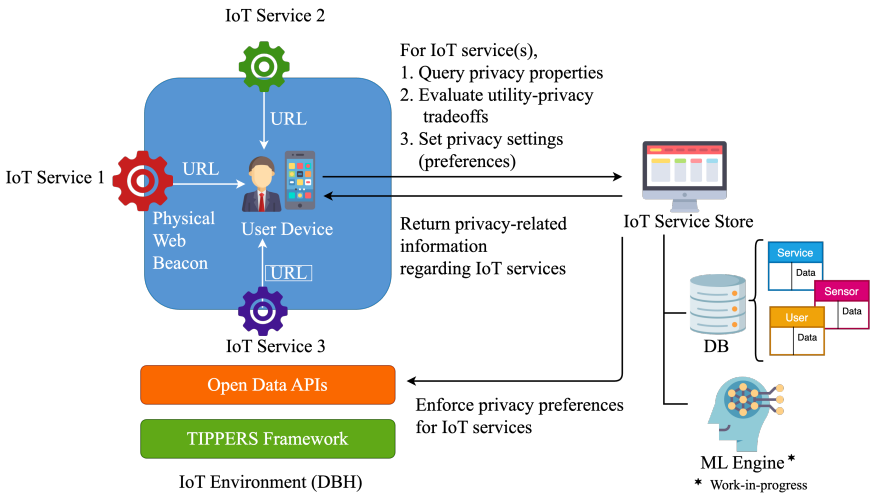


Figure 2.3: IoT Service Store. Adapted from Lee et al. [2018]

Participatory system has components and mechanisms that help people share, search, and publish information from their mobile devices [Lane et al., 2008]. This type of sensing is more active, and users usually perform a designated task [Chi et al., 2018; Pilloni, 2018]. Techniques based on mobile device sensing have advantages over traditional sensor networks, namely low cost, wide-coverage, and high mobility [Gong et al., 2019].

In this category the PiRi framework [Kazemi and Shahabi, 2011] aims to solve the problem of Privacy-Aware Participatory Assignment. The proposal assumes a privacy model where the participants trust each other but do not trust the server. Mistrust in the server stems from the fact that every time a participant wants to execute a task, a query with his location (which generally might include a private address) must be sent to the server, to retrieve a set of nearby places for the execution of the tasks. This process can be used to reveal the main locations of the participant, allowing the user to be tracked.

An extension of this previous the work is the Trustworthy privacy-aware participatory sensing (TAPAS) framework [Kazemi and Shahabi, 2013], which addresses both the privacy and trust issues of participatory sensing. Its objective is to encourage the participation of users without affecting their privacy and, in turn, improve the trustworthiness of the collected data. Another model proposal that offers a solution for assigning tasks to participants without the necessity to reveal their location is proposed by Yuan et al. [2020]. This model adopts a grid-based location protection method along with a hybrid encryption algorithm to preserve the location of tasks and participants.

2.2.3 Privacy Approach

One of the first models capable of providing the user with some control over privacy decisions based on privacy policies dates back to 2002, with the proposal and implementation of the Privacy Awareness System (pawS) for Ubiquitous Computing Environments [Langheinrich, 2002]. For this proposal design, the

author adopts four of the six privacy preservation principles defined by Langheinrich [2001] – Notice, Choice and Consent, Proximity and Locality, Access and Recourse – to elicit the requirements, which are later translated into prototype functionalities. PawS generates privacy beacons announcing the data collection of each of the services, along with the privacy policy, using Bluetooth or Infrared Data Association (IrDA) technology. These beacons are processed by a Privacy Assistant (PA), which resides on the user's personal device. The PA delegates the contact with the Service Proxy (SP) to the Privacy Proxy (PP), which requests the privacy policy and is able to compare it with the privacy preferences established by the user, to accept or decline the service. In this proposal, the privacy policies are encoded in machine-readable XML, and they include the procedures for data collection and the future use of it, for example, who is collecting the data, what kind of data, for whom, and why. From the user's side, the privacy preferences can be defined using APPEL [Cranor et al., 2002], a machine-readable language used for privacy policies.

Chow [2017] proposes the Privacy Stack, a four-layer conceptual model that globally outlines and synthesizes the functionalities and characteristics that a privacy-aware IoT system should possess. The four layers composing this stack are Awareness, Inference, Preferences, and Notification. The first layer encompasses everything related to the communication channel opening by the IoT service to users, and how they manage to discover the privacy properties of these services. The communication channel can be established through visual signifiers or through traditional network protocols between the service and the user. The second layer tackles the limited knowledge that a user might have about the information that can be inferred from the captured data. For this point, the author proposes that IoT services must expose the basic inferences through privacy policies. The Preferences layer shows that the user is the entity in charge of making the privacy decisions regarding a particular IoT data collection scenario. However, these decisions must depend on the context. Finally, the Notification layer is the one related with the user interaction. The notification mechanisms that are deployed from it must be based on the results of the previous layers, for the user to find them useful without becoming annoying. In addition to notifications, the author leaves open the possibility of other types of interactions, for example, the display of privacy policies and the setting of privacy preferences by the user through a privacy proxy.

In Wang et al. [2013], the privacy preferences' definition is also made on the user's handheld device, while each IoT resource is in charge of the privacy policies' provision. The privacy policies can be managed by a central infrastructure in charge of their distribution, as in the case of the privacy preference model for IoT applications proposed by Cha et al. [2018], called Privacy Bat, based on Bluetooth Low Energy (BLE). This model provides a method and a format for IoT devices management, allowing the registration of the devices along with their privacy policies. On the user side, the model defines a standard way for privacy preference notifications toward BLE devices. In this model the Device Information Service (DIS) stands out as the core component. DIS implements two interfaces. The first interface, called Device Registration and Management, is responsible

for the registration and management of IoT devices. For the registration, the administrator identifies each of the devices using a 128-bit Universally Unique identifier (UUID). Each IoT device must periodically broadcast its identifier using BLE. The moment the user's device captures a beacon, DIS is contacted through the second interface, called Device Information and Privacy Policy Provision, to obtain the privacy policies associated with the IoT device. Once the privacy policies have been received, the user can express his/her privacy preferences through the Privacy Preference Expression Generic Attribute Profile (GATT) Service, accepting or rejecting the IoT device policies. This model implements the Platform for Privacy Preferences (P3P) [Cranor, 2003], relying on the definition of privacy policies by the DC, who is responsible for data collection and its subsequent use. The model also establishes the means for the DS to access their information. For the validation of Privacy Bat, the authors implemented a proof-of-concept through a centralized system.

Inspired on Pappachan et al. [2017], Das et al. [2018] consider that there is a pressing need to implement a model capable of discovering and obtaining information about IoT resources (devices, services, and applications) around us, that may collect and use our data without our explicit consent. This infrastructure prototype was implemented and deployed in the Carnegie Mellon University campuses. It is made up of three main components, the IRR, PPA for IoT, and the Policy Enforcement Point (PEP).

IRRs allow IoT resource owners to provide descriptions of resources, including the purpose of data collection, retention period, and the third-party data sharing police. The PPA is an application for smartphones that assists users in the IoT resource discovery process, based on their location. However, the PPA is limited to only listing the available resources registered in the IRRs. It should be noted that the information that the PPA deploys is based on the privacy preferences previously established by the DS. Lastly, the PEP is responsible for controlling the collection and use of data according to the privacy settings. This component oversees verifying that the data obtained through the IoT resource is processed as established by the user. The PEP component can be embedded in the IoT resource or implemented as an external proxy. The IoT resource registration with an IRR is performed through a portal, where the resource owners must authenticate themselves. The registry can be executed from scratch or by custom templates with predefined values. After this process, the PPA installed in the user's smartphone can discover the published IoT resources and configure some privacy settings through interaction with the application. Finally, the PEP enforces the privacy settings of each user when IoT resources start collecting data. This IoT infrastructure is an extension with a very similar approach to the proposal presented in Das et al. [2017] in the field of privacy-oriented facial recognition, where users are warned about the presence of smart cameras in their whereabouts.

Halcu et al. [2015] propose a privacy model for HiTLCPS guided by the privacy-aware design principles introduced in Wicker and Schrader [2011]. The Privacy/Security Engine in one of the components of the model and acts as an intermediary between the Data Provider and the Data Post-Processing within

the pre-processing stage, anonymizing the data and considering the Privacy Policies defined by the user. Those policies include restrictions in sharing location, notifications, and tracking. Also, this model defines the use of Transport Layer Security (TLS) connections, an anonymous authentication scheme based on certification messages and a privacy rule generator for the HiTL control based on the emotion classification and the user's feedback. In this model the authors define two privacy levels namely Low Level and High Level. The former is directly related to negative emotions while the latter is associated to positive emotions. For both levels, there is a set of actions and settings that are configurable by the user.

A generic framework for consent and information in IoT was proposed by Morel et al. [2019]. The underlying technical functional requirements are based on the recommendations established by GDPR [Parliament et al., 2016] and on the published guidelines on transparency and consent of the Working Party 29 (WP29) [Commission, 2016; Party, 2018]. In this model, the interaction between DC and DS is defined, and divided into two parts, the first between the DS and its Gateway Device, and the second between the Gateway Device and the DC device. The privacy policies definition and semantics are based on what is stated by Pardo and Le Métayer [2019]. Within the technical options, this framework considers two possibilities: the first one is direct communication between DC and the DS devices (Gateway Device and other devices), and the second one is indirect communication using registers. Direct communication can be implemented using wireless communication technologies, such as Bluetooth or Wi-Fi, without an internet connection and without affecting other services. On the other hand, indirect communication requires the implementation of registries, used by both, DC and DS. In the case of DC, the registry will be a privacy policies repository, to which DS can access regardless of their location, minimizing the risk of location inference through direct communication. However, having indirect communication requires a periodical record update by DC. DS-side records can be implemented for DC to access the provided consents. However, this option is weaker in terms of privacy, since DS must disclose their privacy policies. Finally, within the model, the authors also define an element called Personal Data Custodian (PDC), which is essentially software for the DS Gateway Device. This software allows DS to consult the information retrieved from DC and to express privacy preferences. PDC interact with DC for allowing or denying data collection.

Another approach similar to the previous one is proposed by Lee et al. [2019] where the DC asks the DS for consent for personal information collection. Unlike other contributions, the information exchanged between DSs and DCs is encrypted using asymmetric keys. The privacy preservation model includes four elements within the interaction: the user's IoT device, the user's agent, the Gateway device, and the data collection server. The IoT device and the user agent make up the DS, while the Data Collecting Server represents the DC. The Gateway device works as the intermediary between the DC and the DS. Within this proposal, the format of the messages to be exchanged between DS and DC is defined. The interaction defined in this procedure begins with the

sending of the Personally Identifiable Information (PII) Message by the User IoT Device. In this message, each type of PII is encrypted with a different public key, in addition to containing the public key of the DS. Once the message has arrived, the DC selects which PII requires, and requests consent from the User Agent by sending it an encrypted consent message with the DS public key. The consent request message includes the Device ID, DC certificate and the privacy policy document. The former element is displayed to the DS through the User Agent. The DS is going to select and check the items in the collection list that are allowed for the DC. in the case of approving the collection, it encrypts the private keys using the public key of the DC and sends the consent message. Once the message is received, the DC can decrypt the fields of the PII to which the DS allowed access. It is worth mentioning that this procedure has not been evaluated in a real scenario nor through a prototype.

Sun et al. [2020] propose iRyP a purely edge-based privacy-respecting system for mobile cameras where the DS privacy preferences are piggybacked into the BLE advertisement messages. In this proposal DSs define their privacy preferences offline and then upload it to their smart devices. Once the smart device contains the privacy profile, this is going to be broadcast to other smart appliances with camera capabilities for privacy enforcement. Similarly, Rios et al. [2022] propose a distributed Privacy Manager system based on Edge Computing (PMEC), to handle personal IoT devices in extended home ecosystems. The privacy preferences are expressed based on a context-aware policy language to aid DSs in this task. Through these preferences is possible to define the data access and data management privacy policies.

An augmented reality based privacy management interface is proposed by Bermejo Fernandez et al. [2021]. This model called Privacy Augmented Reality Assistant (PARA) serves as a privacy-preserving assistant specifically designed for smart devices in a home environment. The main goal of PARA is to provide real-time contextualization of data disclosure to users and empower them to control their privacy preferences through the utilization of privacy filters.

Barhamgi et al. [2018] present a vision of how DSs will have a central and effective role in protecting their privacy within a cyber-physical environment, through the proposal and implementation of a data exchange architecture. This implementation allows DSs to evaluate implicit privacy risks and contrast them with the benefits of information sharing. The proposed solution can be adapted to the IoT environments context. Additionally, this proposal analyzes the requirements that future data collection architectures must implement to provide effective protection in terms of privacy. The first requirement is related to capability for users to understand privacy risks, given the subjectivity of their vision, in addition to having the necessary mechanisms to control the exchange of information. The second requirement is that there must be a pragmatic stance from the user, being able to assess the risk and balance it against the benefits established by the DC and, if necessary, to negotiate before starting the data exchange process. Finally, it is recognized that the decision to share data may depend on the context of the DS and, therefore, the architecture must detect possible context changes to take necessary actions. In addition to the architec-

ture depicted in Figure 2.4, the authors propose a model capable of balancing the exchange of information based on risks and benefits. To calculate the risk, the query sensitivity, the degree of confidence in the DC, and the potential information leakage in the case of answering the query are considered. In the case of profit measurement, this proposal is still very subjective. Similarly, in Markovic et al. [2018], an IoT privacy risk assessment service is proposed, which evaluates the input information based on a risk model that takes into account the parameters of the IoT device, the communication channel, and the data storage location.

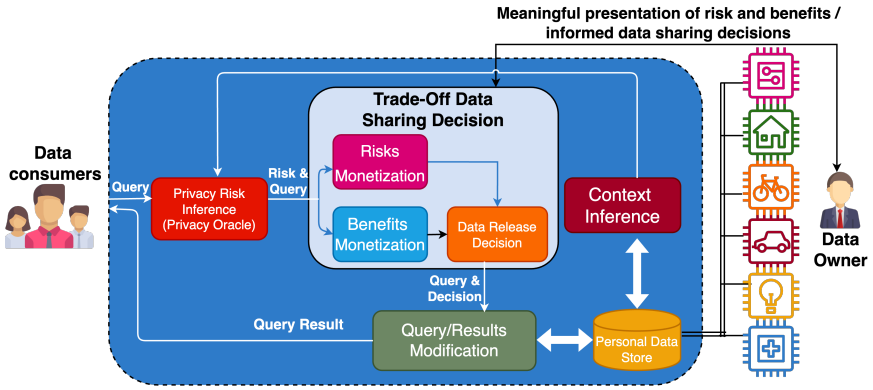


Figure 2.4: An architecture for user-centric privacy preservation for the IoT. Adapted from Barhamgi et al. [2018]

It is also worth mentioning that some models adopt a dual approach, where both approaches are proposed and implemented within their architecture, as is the case of the model presented by Torre et al. [2016b]. In this contributions the authors introduce a framework for personal information protection that integrates a Personal Data Manager (PDM) and an Adaptive Inference Discovery Service (AID-S) [Torre et al., 2016a]. These two components form a block labelled as [PDM + AID-S], placed between the user and third parties. Among the PDM functions, the main one is privacy policies or policy statements revision from IoT Services and third parties, to maintain consistency with the users' privacy settings prior to the decision to access the information. On the other hand, AID-S calculates inference risk associated with the disclosure of personal information. [PDM + AID-S] comprises five functionalities –managing the interaction among parties, access control, recommendations, inference discovery and user profiling– composed of eight tasks –Dialog management, Authentication/Authorization, Policy statement evaluation, Privacy Preferences settings, Privacy Preferences and thresholds estimation, Inference risks computation, Optimal privacy setting, and Transformation to sanitize shared data–. The PDM delegates communication coordination to the Dialog Management task, by using dedicated interfaces between the user (PDM2User), third parties (PDM2Third-Party), and AID-S (PDM2AID-S). For the access control functionality, there are two tasks. The first one addresses the request evaluation from third parties, based on Privacy Statements containing information that describes what data will be collected, processed, and stored, the quantity and frequency, and the possible uses. The second task, named Authentication and Authorization, is done

by managing a list of authenticated third parties. Third party authorization is given once the request is certified and accepted. To carry out the evaluation of third-party requests, the PDM creates user profiles where privacy preferences are declared and configured. There are some PDMs which partially implement the tasks shown in this framework, such as Databox [Chaudhry et al., 2015], Enigma [Zyskind et al., 2015], and ipShield [Chakraborty et al., 2014].

Similarly, in the privacy management model described by Psychoula et al. [2017], when a DC wants to access the user data collected in a smart home context, the request must pass through a Privacy Risk Detector. This component along with the Privacy Management component estimate the requested data sensitivity based on the privacy preferences established by the DS and implement an access control feature to allow or denied the access to the data, according to the access level of the DC. All the allowed data is anonymized before being accessible by the DC. This model was assessed using a case study comprising 16 smart homes equipped with ambient sensors and actuators.

Data Bank is proposed by Jaimunk [2019], as a model to manage data from IoT devices and control its transfer to cloud services. This proposal provides the DS and the DC with a model to declare data collection policies and data sharing policies respectively. The architecture of this model comprises three main features namely data repository, privacy-utility mechanism, and access control enforcement. The first feature allows the data to be store locally in a component called Data Pocket before transferring to the data repository in the cloud. This component keeps the predefined privacy policy and filter's user data. The second feature looks for finding the right balance between benefits against possible privacy lost. Finally, access control enforcement restricts DC to access to the DS's data based on an access control policy.

2.2.4 Model Architecture

Thus far, the majority of the examined models exhibit a centralized architecture, wherein a prominent intermediary component assumes a crucial role. These mediators primarily serve to coordinate data protection-related operations and processes. For instance, in Pappachan et al. [2017], TIPPERS serves as the convergence and management point for services, sensors, and policies. Similarly, in Das et al. [2018] this role is assumed by the IRR. A similar pattern emerges in Lee et al. [2018], where the ISS facilitates service management and enforces privacy preferences.

Although the centralized proposals are the majority group in this review, over the years, there has been a gradual shift from these approaches to decentralized proposals. As the proliferation of connected devices continues to expand, the reliance on a centralized infrastructure for data processing, storage, and decision-making has become increasingly impractical and prone to single points of failure. Acknowledging these challenges, the scientific community and the industry has started to embrace decentralized approaches as a promising solution

Notably, Rantos et al. [2019] and Agarwal et al. [2020] leverage blockchain

technology to ensure consent integrity and versioning respectively. The first approach, called ADVOCATE, presents a user-centered solution for handling provisioned consents, validating them, identifying conflicts between rules and policies, and assisting DS in making appropriate privacy decisions. Conversely, the second framework named Consentio, primarily focuses on a consent management model based on a permissioned blockchain. In this proposal, the consent management process is decoupled from the data management process, and the consent is jointly managed among the involved parties.

Alhajri et al. [2022a] propose a blockchain-based consent mechanism for accessing fitness data in a healthcare context. The designed model strives to meet multiple requirements, including transparency, security, scalability, auditability, preservation of original functionality, and compliance with data protection regulations. The authors present an architecture that incorporates various participants and actions. To validate security requirements such as authentication and proof of authenticity, they rely on a security modeling framework called SeMF.

The model presented by Saha et al. [2020] focuses on IoT applications in the healthcare sector, where the privacy and confidentiality of DS's data are of paramount importance. To achieve this, the model utilizes a private blockchain to devise an access control scheme. Under this scheme, every new DS is required to authenticate themselves with the trusted Hospital Authority. By adopting such an approach, the model ensures the anonymity and un-traceability of the DS, thereby safeguarding their sensitive information. Similarly, Saha et al. [2021] propose a novel consortium blockchain-based access control scheme that primarily targets edge devices. In addition to supporting access control functionalities, this scheme also facilitates key management between edge devices and cloud servers, specifically within the DC infrastructure.

Manzoor et al. [2021] propose a hybrid model aimed to tackle the issue of one-time consent in centralized consent management and relies on a proxy re-encryption scheme to ensure secure and anonymous transfer of IoT data. This model leverages blockchain technology to tackle scalability, trust issues, and automate payments for shared data, thus addressing additional challenges in the IoT data ecosystem.

Another hybrid approach for data sharing is proposed in Lin et al. [2021] in the scope of sensing-as-service in smart cities. This model integrates some cryptographic techniques such as symmetric and asymmetric encryption schemes, and a signature scheme. According to the authors, their model meets identity management, key renewal, pseudonymity, confidentiality, traceability, fairness and universality challenges.

Egala et al. [2021] proposed Fortified-Chain, a novel model for decentralized healthcare CPS, that includes a Selective Ring-based Access Control (SRAC) mechanism, device authentication algorithms and also aims to preserve DS anonymity. Each table record is a ring for a particular DS. Each entry in the table is referred to as a 'ring' specific to a particular patient. The DS is given the ability to generate multiple distinct static rings for various files. Simultaneously,

based on the index value, the patient can establish a dynamic ring to accept valid file access requests from a remote location. For different categories of files, the patient assigns different index values based on critical information. The SRAC compares the requester's index value with the required index value in the ring to grant secure read-only access to remote actors. Each hospital independently calculates the local actor index values for dynamic file access control. The model is implemented and assessed based on a logical analysis.

At this point and after reviewing the most relevant contributions in this area, it is worth emphasizing two aspects. The first one is that the reviewed models are not category-exclusive in the taxonomy. They were ordered in this section according to its predominant category. However, they can be classified into one or more groups based on their features and the approach they implement, as shown in Table 2.1. The second aspect is that the models we have reviewed, while providing openness for user interaction, also have their own privacy and security mechanisms, such as encryption, anonymization and/or access control. Table 2.1 presents this information for those models that explicitly mentioned the use of any of these mechanisms.

2.3 Open Challenges and Research Opportunities

In the previous section, user-centric privacy-preserving models was thoroughly reviewed. In this section, we are going to synthesize and discuss those contributions, and identify the open challenges and research opportunities that arise from them. The analysis of the literature carried out so far in the current survey shows that some of the challenges identified in early proposals have been addressed in more recent contributions. Nevertheless, we can still identify several directions and considerable challenges to be approached by future research.

For the sake of organization and clarity, we are going to discuss the proposals and identify open challenges based on some common aspects that these models offer, namely:

- privacy preferences and privacy policies management;
- notice and discovery mechanisms;
- consent management;
- risk inference;
- enforcement points and compliance;
- user engagement and incentives
- real scenario deployment and assessment.

2.3.1 Privacy Preferences and Privacy Policies Management

User Privacy Preferences establishment and Privacy Policies declarations are examples of functionality common to several of the revised proposals. In Langhein-

Table 2.1: User-Centric Privacy Preserving Models

Contribution	Smart Domain				Data Acquisition Approach		Privacy Approach			Model Architecture			Privacy Preservation Mechanism	AI Assisted	Validation Approach
	Smart Cities	*Smart Buildings*	*Smart Homes*	*Smart Phones*	*Opportunistic*	*Participatory*	*Privacy Policies*	*Privacy Risks*	*Dual*	*Centralized*	*Decentralized*	*Hybrid*			
Barhamgi et al. [2018]	✓	✓							✓	✓			A-DP		Prototype
Lee et al. [2018]		✓			✓				✓	✓			AC-E	✓	Prototype
Martínez et al. [2017]	✓						✓			✓			E-AC		Prototype
Banerjee et al. [2019]	✓		✓							✓			E-AC		Simulation
Kumar et al. [2019]	✓	✓								✓			E-AC		Prototype
Makhdoom et al. [2020]	✓				✓						✓		AC		Prototype
Pappachan et al. [2017]		✓				✓	✓			✓			A-AC		Prototype
Chhetri and Genaro Motti [2022a]			✓		✓		✓			✓			AC		Prototype
Zavalyshyn et al. [2018]			✓				✓			✓			AC-E-A		Prototype
Muhander et al. [2022]			✓										N/S		Prototype
Wijesundara [2020]			✓				✓			✓			N/S	✓	Theoretical
Keshavarz and Anwar [2018]			✓				✓			✓			AC	✓	N/S
Kounoudes et al. [2021]			✓			✓							N/S	✓	Prototype
Liu et al. [2018]			✓										DP		Simulation
Datta et al. [2018]			✓		✓								DO		Simulation
Xu et al. [2018]			✓							✓			DP		Simulation
Xu and Zhu [2015]				✓									AC		Prototype
Bai et al. [2017]				✓									AC		Prototype
Liu et al. [2016]				✓	✓		✓						N/S	✓	Prototype
Wang et al. [2013]	✓				✓		✓			✓			N/S		Prototype
Kazemi and Shahabi [2011]						✓	✓						A		N/S
Kazemi and Shahabi [2013]						✓							A		Simulation
Yuan et al. [2020]						✓				✓			E		Simulation
Langheinrich [2002]		✓					✓			✓			AC		Prototype
Chow [2017]		✓	✓	✓			✓						N/S	✓	Theoretical
Cha et al. [2018]		✓			✓		✓			✓			AC		Prototype
Das et al. [2018]		✓			✓		✓			✓			AC-A	✓	Prototype
Das et al. [2017]		✓			✓		✓			✓			AC-DO		Prototype
Halcu et al. [2015]							✓			✓			E-A	✓	Prototype
Morel et al. [2019]					✓		✓			✓			AC-A		Prototype
Lee et al. [2019]							✓			✓			E		N/S
Sun et al. [2020]				✓			✓						DO	✓	Prototype
Rios et al. [2022]			✓				✓						AC		Prototype
Bermejo Fernandez et al. [2021]			✓				✓						AC-DO	✓	Prototype
Markovic et al. [2018]			✓					✓		✓			E-AC		N/S
Torre et al. [2016b]			✓		✓				✓				AC		N/S
Psychoula et al. [2017]			✓				✓		✓	✓			A-AC		Theoretical
Jaimunk [2019]					✓				✓	✓			AC		N/S
Rantos et al. [2019]	✓				✓		✓				✓		AC		Prototype
Agarwal et al. [2020]	✓				✓						✓		AC		Prototype
Alhajri et al. [2022a]	✓				✓		✓				✓		AC		Theoretical
Saha et al. [2020]	✓				✓						✓		E-AC		Theoretical
Saha et al. [2021]	✓										✓		E-AC		Prototype
Manzoor et al. [2021]	✓				✓							✓	E-AC		Prototype
Lin et al. [2021]	✓						✓					✓	E-AC		Prototype
Egala et al. [2021]	✓				✓							✓	E-AC		Prototype

(E) Encryption, (A) Anonymization, (AC) Access Control, (DO) Data Obfuscation, (DP), Differential Privacy

rich [2002], privacy preferences are managed by the personal privacy proxy, while the privacy policies are handled by the service privacy proxy. Similarly, in Zavalyshyn et al. [2018], the DS can establish this privacy preference using a management interface of the HomePad. In the case of the models from Pappachan et al. [2017] and Das et al. [2017], privacy preferences are defined in the IoTA and the PPA modules respectively, while the privacy policies of the IoT resources are managed by IRRs. In the model proposed by Lee et al. [2018], the ISS stores the IoT services' privacy policies and allows users to set-up their privacy preferences.

In Cha et al. [2018], a service called Privacy Preference Expression GATT is used to communicate the privacy policies of a device. However, in this model, the preferences are not defined by the user, and the privacy policy evaluation

leads to the consent. In Morel et al. [2019], two possible communication scenarios are contemplated, each one implementing its own type of privacy policy management: in direct communication, the DC privacy policy is sent by the system to the DS smartphone, while in indirect communication, privacy policy management is based on the use of registries. In Torre et al. [2016b] the functionality called User Profiling, which is shared between the PDM and the AID-S, defines the configuration of the users' privacy preferences. In this model, third parties never share their privacy policy.

Setting privacy preferences or access control policies is a challenge as in Martínez et al. [2017] and Wijesundara [2020], especially for people who are not familiar with this area. Therefore, assistance features for this type of configuration should be included in future proposals. In Keshavarz and Anwar [2018] and Das et al. [2018], the authors propose the use of ML models to reduce user burden and also to establish a common taxonomy to describe data collection and use practices. The idea proposed by Lee et al. [2018] is based on the prediction of future decisions and on a historical record of interactions, using ML models. The use of technology based on Artificial Intelligence (AI) in privacy policies is encouraged by Lippi et al. [2019], as a preliminary analysis and legal evaluation could support DSs in identifying unlawful clauses and potential threats.

Morel et al. [2019], argue that improving Graphical User Interfaces (GUIs) would allow DSs to establish these configurations in a better way. Similarly, solutions should be considered for DCs, assisting them in properly declaring privacy policies. Pappachan et al. [2017] propose the development of abstract models for the specification of privacy policies in different contexts. Chow [2017] proposes the idea of context-based privacy preference generators and the privacy metadata standardization for policy declaration, to reduce the cognitive burden for decision making. A way forward can be to take advantage of the HiTL concept, as in Halcu et al. [2015] or using a Privacy Profiles and Recommendations through a PPA as in Liu et al. [2016].

2.3.2 Notice and Discovery Mechanisms

Notice, also known as the principle of openness [Langheinrich, 2001], establishes that systems should notify their users about the services and IoT devices that are around them, as well as the data collection practices, expressed in the form of privacy policies. Thus, the mechanisms and the announcement formats must be defined. Some of the reviewed proposals cover this principle. For instance, in Langheinrich [2002], the use of Bluetooth or IrDA technology for advertising, and P3P as the selected format for privacy policies, are contemplated. In Pappachan et al. [2017] and Das et al. [2017], a central registry is used as a repository, known as IRR, where privacy policies are declared by the system administrator or by IoT service providers, and propagated using Bluetooth beacons. These beacons are subsequently received by the users' mobile device. Similarly, the framework proposed in Lee et al. [2018] uses Bluetooth beacons.

However, in the latter proposal these frames only contain an identifier for a subsequent connection with a server where the privacy policies are stored. In

Cha et al. [2018], the authors propose the use of BLE for propagation, and P3P for the policy format. The framework proposed in Morel et al. [2019] mentions the possibility of using both registers in the style of the proposals presented by Pappachan et al. [2017] and Das et al. [2017], as well as BLE technology and Wi-Fi for the policies announcement. In Torre et al. [2016b] and Barhamgi et al. [2018], there is no mention to any mechanism for announcing or discovering IoT resources. This principle is specifically addressed in Chow [2017], both in the awareness layer and in the notification layer of its conceptual model.

IoT resources discovery and initial exchange of information with the user is a challenge, especially in ubiquitous environments, where the advertisement of services of this nature is distributed. Current solutions propose the use of centrally managed records, or the diffusion of broadcast messages using wireless technology. However, a unified way of carrying out this task has not been defined, as suggested by Pappachan et al. [2017], which also mentions the need to work on new models for user notification. In this revision, we observed that most frameworks declare their presence using Bluetooth or BLE as the enabling-technology. However, their solutions have not been tried and tested with other types of wireless schemes. So, establishing a comparison with other protocols would be desirable in the quest for a standard solution. An alternative to overcome compatibility problems is proposed in Lee et al. [2018], by implementing a gateway (Gate-Keeper) for legacy BLE devices that do not support the framework.

2.3.3 Consent Management

In most implemented models, consent is derived from the relative weight of the privacy policies and the preferences established by the DS. The framework developed by Langheinrich [2002] delegates to the PP the task of granting a sort of consent, after considering preferences and policies. In Pappachan et al. [2017] and Das et al. [2017], consent is granted through a PPA running on the user's smartphone. However, in those proposals the consent management definition is not explicitly addressed. Something very similar happens in Morel et al. [2019], where, besides the PDC, this model allows the management of previously granted consents.

Regarding automatic consent, Colnago et al. [2020] discuss that this is one open issue arising from the use of PPAs. Users tend to perceive automatic consent negatively as it limits their sense of control. The authors propose a solution of keeping the data in custody during the data DS review process. However, this approach may introduce challenges in handling time-sensitive requests.

In Lee et al. [2018], information collection permission is given at subscription time to an IoT service, while in Cha et al. [2018] the user grants or denies the consent once the privacy policy has been received by IoT device. In the conceptual framework proposed by Chow [2017], the third layer of the model encompasses this principle. In the case of the proposals presented by Barhamgi et al. [2018] and Torre et al. [2016b], the delivery of explicit consent for the collection of information is not addressed.

Like the discovery of IoT resources, obtaining and managing consent is a critical process. In Morel et al. [2019], the implementation of authentication mechanisms to ensure the integrity and authenticity of consent is proposed as future work by using a secure ledger to store the granted consents and thus safeguard their integrity.

Blockchain technology and consent management are crucial in today's digital landscape. The importance of blockchain lies in its ability to provide transparency, immutability, and security in managing consent [Peyrone and Wichadakul, 2023]. By leveraging this technology, organizations can create decentralized and tamper-resistant systems for recording and managing consent-related transactions. This empowers individuals to have control over their personal data, ensuring that their consent is obtained and respected in a verifiable manner [Rantos et al., 2019].

Several models rely on a combination of blockchain and cryptographic techniques like proxy re-encryption for consent management and data sharing [Manzoor et al., 2021]; however, one main concern in this approaches is the possibility of collusion attacks. In this sense some contributions like Obour Agyekum et al. [2019], Guo et al. [2021] or Lin et al. [2022] propose enhancing this cryptographic scheme with novel techniques that can be incorporated and must be validated in future user-centric privacy-preserving models.

Moreover, for data sharing tasks directly related with consent management processes, effective authentication, access control and key agreement mechanisms ensures that only authorized individuals or entities can interact with IoT devices and access the data they generate and acquire. This safeguards against unauthorized access, data breaches, and potential misuse of sensitive information. In this sense, the models proposed and assessed through security analysis in Banerjee et al. [2019]; Saha et al. [2020, 2021]; Sutrala et al. [2022]; Alhajri et al. [2022a,b], are paving the way for more secure and reliable future implementations in the user-centric IoT scope.

2.3.4 Risk Inference

Based on the information provided by IoT resources, and after some processing, additional information can be inferred, without DSs being aware of this. Some of the reviewed models address this problem. In the model proposed by Lee et al. [2018], information given to the users about IoT services includes inference types that can be performed based on the collected data. The framework presented by Kounoudes et al. [2021] is able to notify the user regarding unwanted inferences based on environmental data collected by smart home devices. In Torre et al. [2016b], the framework allows inference risks calculation before disclosing personal data, as in Barhamgi et al. [2018], where, in addition to the calculation of the risk, there is also a context inference module. In the framework presented by Chow [2017], one of its layers includes the handling of inferences, while the proposal in Corcoran [2016] delegates to the industry the responsibility of establishing guidelines to minimize risks.

Improving personal information's inference based on sensor data is one of the challenges mentioned in some of the reviewed articles. According to Lee et al. [2018], this is a complex task, highly context-dependent, and subject to considerable misunderstandings. In this article, the authors propose a probabilistic information retrieval system to derive relationships from sensor data and personal information. Likewise, in Barhamgi et al. [2018], the development of models and techniques for the representation and monitoring of context related to user privacy that can detect modifications is identified as a challenge. User interactions with the environment must also be further studied.

2.3.5 Enforcement Points and Compliance

An enforcement point is an entity that ensures privacy preferences set by the user will be respected. From the group of the reviewed models, only those proposed by Das et al. [2018], Pappachan et al. [2017], and Lee et al. [2018] contemplate this feature. Das et al. [2017] includes an element known as PEP within its architecture, which can reside in the IoT resources or be implemented as an independent element. In Lee et al. [2018], the authors provide and propose the use of an enforcement engine.

Another proposal that includes an enforcement element, although it is not a User-Centric IoT framework, is the 'VisiOn Privacy Platform' by Diamantopoulou et al. [2017]. Apart from the Privacy Level Agreement (PLA), which is essentially a contract between DC and DS, the Privacy Runtime component controls the data access request, and enforces the data access policies generated automatically based on system models information and DSs' privacy preferences.

To achieve timely control of compliance with the privacy preferences of the DS by DCs, in Pappachan et al. [2017], the authors propose to work on the optimization of the control process for privacy policies, with reference to the privacy preferences established by the user and in Lee et al. [2018], the idea of a vetting system in IoT devices is suggested, to verify how personal data is managed.

One possible approach to evaluating the compliance of privacy policies with data protection regulations is through the use of AI-based technologies namely ML and Natural language Processing (NLP), as advocated by Lippi et al. [2019]. This approach references CLAUDETTE [Contissa et al., 2018], an automatic detection component that identifies potentially unfair clauses in online terms of service. Furthermore, CLAUDETTE can also be applied to privacy policies to assess their compliance with the GDPR.

2.3.6 User engagement and Incentives

An important aspect of participatory and opportunistic sensing is the incentives in exchange for performing a task or registering into a service [Bobolz et al., 2020]. In Jin et al. [2018], a model called INCEPTION integrates mechanisms for incentives, aggregation, and data disturbance. The incentive mechanism

is based on reverse auction to compensate the workers, while the aggregation and disturbance mechanisms of the data aim to increase the reliability and precision of the sensed data and, therefore, protect the workers' privacy. In Gong et al. [2019], the Privacy-Aware Task Assignment Framework (PATA) includes incentive mechanisms, similarly to the ones in Jin et al. [2018]. This model publishes the set of tasks to be executed, including their position and the incentives associated with them. Based on the workers density, the incentive is determined. Users who are within the range where tasks have been released can choose which tasks are more convenient according to their profile. Although, this framework does not declare a mechanism for data disturbance or anonymization, it is understood that the user has the power to choose the task that most closely aligns with his privacy profile. A user location privacy-aware incentive model is proposed by Koh et al. [2017], to promote users' participation in sensing tasks and therefore increase the range of dataset coverage. The privacy approach adopted by this model is based on cloaking regions to obfuscate the workers' precise location.

From the list of reviewed models only Liu et al. [2016] explicitly cover some strategies for engagement such as example simplified controls, enhanced awareness and privacy nudges. However, despite the good engagement achieved with the privacy nudges, the authors argue that only a 5.1% of privacy settings were modified by the DS after these notifications. Also, they consider that micro-interaction at appropriate times and tailored the context of the DS could increase the usability of this strategy.

Related to consent management, Peyrone and Wichadakul [2023] state that future work must include incentive mechanism to assess DS compensation against data sharing cost and balance incentives for all stakeholders.

2.3.7 Real Scenario Deployment and Assessment

The frameworks presented by Das et al. [2017] and Pappachan et al. [2017] have been deployed at the Carnegie Mellon University and the University of California Irvine, respectively, as part of the TIPPERS[1] and Privacy Assistant[2] projects. The study presented by Cha et al. [2018] implements a proof of concept. Similarly, in Morel et al. [2019], the authors establish a direct communication prototype based on BLE Privacy Beacons within the "Bluetooth-based tracking" case study. The model proposed by Barhamgi et al. [2018] was put into practice through a case study for the monitoring of twenty chronic patients aged between 20 and 67. In the case of PMEC, Rios et al. [2022], provide to the community a proof-of-concept implementation of their Privacy Manager Instances (PMI) however it does not include Peer–to–Peer (P2P) protocols for synchronization an negotiation.

For models proposed by Notario et al. [2014] and Senarath et al. [2017], validation is necessary in terms of efficiency, practicality, and alignment with best

[1]http://tippersweb.icsprojects.uci.edu
[2]http://privacyassistant.org

practices and legal constraints in real scenarios. The authors consider that in order to continue refining the frameworks, it is necessary to apply them together with existing, well-established development methodologies. With a perspective oriented to the IoT, and given the lack of specific frameworks for the design of this type of applications and platforms, Perera et al. [2016] propose a model made up of a set of thirty privacy guidelines, based on the eight strategies raised by Hoepman [2014]. The authors argue that these guidelines should not be used to compare different IoT platforms or applications, but to evaluate them and find privacy gaps, since each implementation is designed for a specific purpose. In the case of the consent management framework for fitness data proposed by Alhajri et al. [2022a], one of its main limitations of the is the lack of an experimental evaluation.

User perception is fundamental in user-centric system development and adoption where the main objective is to preserve privacy. Some of these models go a step further empowering users with control over their privacy. However, none of the previously reviewed proposals has addressed this challenge by executing any kind of qualitative study, such as in the case of Chhetri and Genaro Motti [2022a], Chhetri and Genaro Motti [2022b], Worthy et al. [2016], Zheng et al. [2018] and Colnago et al. [2020]. In Lee et al. [2018], it is mentioned that previous studies using hypothetical IoT services do not reveal the true perception of privacy that users have and, therefore, it is necessary to analyze the behavior in terms of privacy within a real scenario. As future work, Cha et al. [2018] suggest the implementation of usability tests to determine users' attitude toward the application, and to improve the experience.

The main features of the addressed models, as well as the open challenges and research opportunities presented in this section, are summarized in Table 2.2.

2.4 Summary

Without privacy, the deployment of user-centric IoT solutions is non-viable. IoT is impacting our lives and, as such, it is crucial to devise and put into place approaches and mechanisms that preserve and guarantee individual rights, of which the right to privacy is one of the most important. The proposal and development of privacy-preserving models and solutions is gaining momentum among the scientific community. Nevertheless, there is still a long way to go in this area, where Human-Computer interaction (HCI), HiTL, ML models, and M2M communication mechanisms will play an important role in privacy preservation within new digital environments.

In the dynamic landscape of privacy and data protection, an array of promising research avenues and challenges have emerged across various domains. Within the area of Privacy Preferences and Privacy Policies Management, innovative ML models have surfaced to alleviate user burden, enhance graphical user interfaces, and generate context-aware privacy preferences. The integration of the HiTL concept and personalized privacy assistants has also gained traction, empowering users with tailored privacy profiles and recommendations. Lever-

Table 2.2: Summary of models, features, current deployments and open challenges

Feature	**Relevant Contributions**	**Current Deployments**	**Research Opportunities and Challenges**
Privacy Preferences and Privacy Policies Management	Langheinrich [2002] Zavalyshyn et al. [2018] Pappachan et al. [2017] Das et al. [2017] Lee et al. [2018] Cha et al. [2018] Morel et al. [2019] Torre et al. [2016b] Martínez et al. [2017] Wijesundara [2020] Keshavarz and Anwar [2018] Lippi et al. [2019] Halcu et al. [2015] Liu et al. [2016]	- Privacy Proxies - IoTA + IRR - PPA + IRR - ISS - Privacy Preference - Expression GATT - PDM and AID-S with User Profiling	- ML models to reduce user burden - Improving GUIs - Context-based privacy preference generators - HiTL concept - Personalized Privacy Assistants (Privacy Profiles and Recommendations) - AI-based models to identify unlawful clauses and contradictory privacy preferences
Notice and Discovery Mechanism	Pappachan et al. [2017] Das et al. [2018] Barhamgi et al. [2018] Lee et al. [2018] Cha et al. [2018]	- Central registry (IRR) - Bluetooth beacons with JSON Schema v4 - Bluetooth beacons with URL - BLE beacons and P3P - IoT Service Diffusion	- Unified discovery mechanism - Taxonomy to describe data collection and use practices. - Abstract models for privacy policies' specifications - New models for user notification - Gatekeepers for legacy devices
Consent Management	Colnago et al. [2020] Lee et al. [2018] Rantos et al. [2019] Morel et al. [2019] Saha et al. [2020] Saha et al. [2021] Alhajri et al. [2022a] Agarwal et al. [2020] Guo et al. [2021] Lin et al. [2022] Manzoor et al. [2021]	- Privacy Proxies Delegation - Consent Provision using the PA (PPA and IoTA) - Granted through the PDC - Several access control mechanisms for decentralized environments and secure authentication protocols for exchanging the sensitive information	- Authentication mechanisms for integrity and authenticity. - Efficient Secure ledgers to store consent - Implementation and assessment of access control mechanisms and novel proxy-re-encryption models for data-sharing tasks - Models for consent revision in time-sensitive request
Risks Inference	Barhamgi et al. [2018] Lee et al. [2018] Corcoran [2016] Chow [2017] Torre et al. [2016b] Kounoudes et al. [2021]	- Inferences in the user devices - Calculation of inference risks - Context inference modules - User notification unwanted inferences	- Probabilistic information retrieval systems. - Models and techniques for context representation and its monitoring
Enforcement Points and Compliance	Das et al. [2018] Pappachan et al. [2017] Lee et al. [2018] Das et al. [2017] Lee et al. [2018] Diamantopoulou et al. [2017] Lippi et al. [2019] Contissa et al. [2018]	- PEP within the infrastructure or in the user device. - Enforcement Engine -CLAUDETTE	-Enforcement Agents - Control process optimization - Vetting systems - AI-based models (ML and NLP) to assess compliance with privacy regulations
User engagement and Incentives	Bobolz et al. [2020] Jin et al. [2018] Gong et al. [2019] Koh et al. [2017] Liu et al. [2016] Peyrone and Wichadakul [2023]	- Simplified controls - Enhanced awareness - Privacy nudges - INCEPTION - PATA	- Micro-interactions in opportune times and based on the user's context
Real scenario deployment and assessment	Das et al. [2017] Cha et al. [2018] Morel et al. [2019] Barhamgi et al. [2018] Rios et al. [2022] Notario et al. [2014] Senarath et al. [2017] Chhetri and Genaro Motti [2022a] Chhetri and Genaro Motti [2022b] Worthy et al. [2016] Zheng et al. [2018] Colnago et al. [2020]	- TIPPERS testbed - Privacy Assistant Project - Bluetooth-based tracking - Monitoring of chronic patients - PrivacyEnhACT - PMEC	- User's perception based on qualitative studies and usability tests - Validation in terms of efficiency, practicality, and alignment with existing development methodologies - People-Centric IoT platforms assessment - Methodology for frameworks' assessment

aging AI-driven techniques to identify unlawful clauses and conflicting privacy preferences is another compelling direction. Meanwhile, the evolution of Notice and Discovery Mechanisms presents an array of challenges, including the need for unified discovery mechanisms, taxonomies for comprehensive data collection descriptors, abstract models for privacy policy specifications, and novel approaches to user notification. Additionally, the landscape of Consent Management beckons for exploration, encompassing aspects like authentication mechanisms, secure ledgers for consent storage, innovative access control strategies, and dynamic proxy re-encryption models.

Risks Inference offers enticing research prospects, prompting the development of probabilistic information retrieval systems and refined techniques for contextual representation and monitoring. On the front of Enforcement Points and Compliance, the potential lies in crafting enforcement agents, optimizing control processes, devising vetting systems, and harnessing AI-powered models for precise evaluation of compliance with privacy regulations. Lastly, regarding Real Scenario Deployment and Assessment necessitates user-centric insights derived from qualitative studies and usability tests, validation encompassing efficiency and practicality, evaluation of People-Centric IoT platforms, and establishment of methodologies for framework assessment. This multidimensional landscape invites researchers to shape the future of privacy preservation.

In this chapter, we have surveyed the state-of-the-art regarding the specific field of privacy preservation in the context of an evolved IoT paradigm. Through a classification proposal, we were able to better understand the scope and features of existing approaches, and to delve into some of their most relevant characteristics. Subsequently, this allowed us to identify and discuss open issues and research challenges, which is crucial for deciding on which way to go. This overall view and analysis of existing work, limitations and challenges is one of the main contributions of this Thesis.

Publications based on this chapter's work

- Rivadeneira, J. E., Silva, J. S., Colomo-Palacios, R., Rodrigues, A., and Boavida, F. (2023c). User-centric privacy preserving models for a new era of the internet of things. *Journal of Network and Computer Applications*, page 103695 **(Q1)**;

Chapter 3

Toward a Privacy-Preserving Model for Human-in-the-Loop Cyber Physical Systems

Contents

The inclusion of human-related aspects in the IoT paradigm leads to the development of models and solutions that address several challenges of our society. The adoption of these novel approaches is expanding rapidly on the road to what is now termed Society 5.0. However, leaving aside all the potential benefits that come from the interaction with these novel systems, an increasing number of people are concerned with the amount of data these systems can collect and share with Data Requesters (DRs). Several legal frameworks call for the adoption of practices regarding data protection and pushing for data control by the data owners. Unfortunately, user-centric IoT-based systems, like those that follow the HiTLCPS concept, lack mechanisms for managing resources and data in the user domain.

In this chapter, we begin by introducing the concept of HiTLCPS and its distinct phases. We explore its fundamental notion, which emphasizes the active involvement of humans in the functioning and decision-making processes of CPS. Following that, we present two approaches to privacy preservation: one focused on the data acquisition phase and another aimed at the state inference phase. With these two approaches we aim to pave the way toward a unified privacy-preserving model for HiTLCPS .

3.1 Human-in-the-Loop Cyber Physical Systems

HiTLCPSs regards humans as a component to the control-loop of a CPS, with applications focusing on the individual over any other element. A HiTLCPS takes into account intentions, actions, emotions, and mental states such as beliefs, and desires. This inner feature enables the creation of intelligent and adaptable advice systems [Nunes et al., 2015]. Leveraging this concept, it is possible to develop services that sway emotions, actions, psychological states, human drives, and motivations as part of larger–scale systems considering not only physical devices but software-based solutions and humans themselves for sensing and actuation purposes.

The process carried out by a HiTLCPS as depicted in Figure 3.1, includes three main phases. The first one is *data acquisition*, which comprises physical electronic-based devices, software-based entities, and human beings by considering activities from OSN. The second is the *state inference phase*, capable of gleaning intents, states, emotions, and actions. Finally, the third phase, *actuation*, seamlessly integrates both human-driven and human-like approaches to deliver actionable feedback and motivational cues to the user. It is important to emphasize that the user can indeed function as an agent of action within the system, either individually or as part of a collective, thus establishing a nuanced parallel with concepts from the realm of particle physics, where the fundamental behavior of particles governs the system's dynamics on both macro and micro scales. This intriguing concept opens the door to exploring a rich spectrum

of possibilities where user interaction shapes the system's behavior akin to the intricate interplay of particles that define the physical universe.

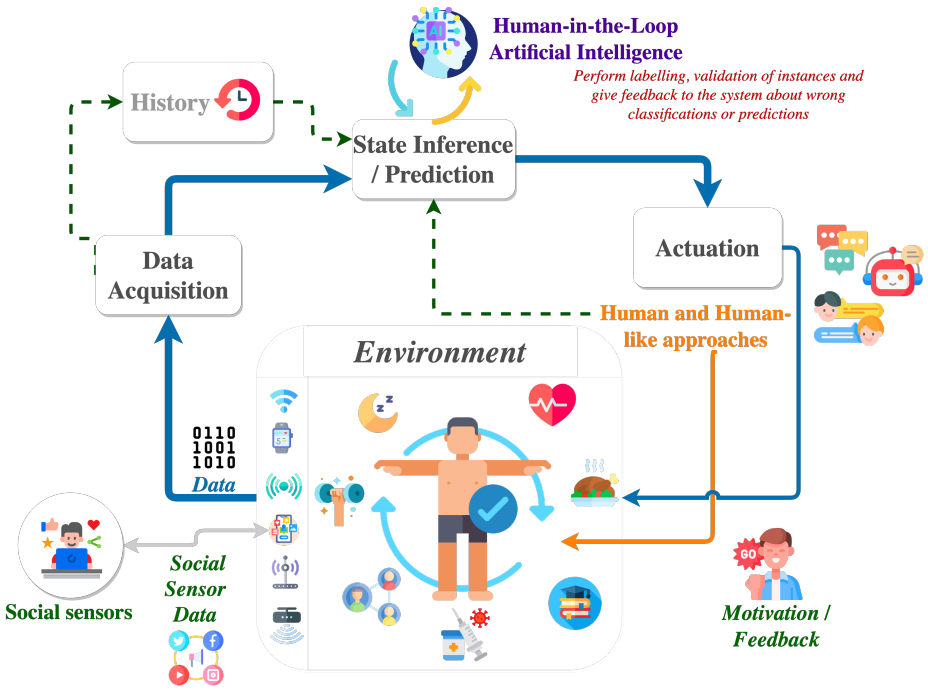


Figure 3.1: An implementation of the HiTLCPS notion in a closed-loop case

This shift in the traditional IoT approach is looking forward to fostering the creation of services that can effectively engage individuals. These services aim to enhance the user's quality of life by providing personalized assistance. However, to ensure their effectiveness, integration of IoT data analytics and AI mechanisms becomes imperative to deliver accurate feedback, precise assistance, and tailored recommendations.

The implementation of systems grounded in this notion introduces a host of challenges, chief among them being the imperative preservation of the privacy of the human factor. Our conception of the distinct phases comprising a HiTLCPS reveals a significant insight: privacy considerations hold the greatest prominence in the data acquisition and state inference phases. This strategic perspective is underpinned by several factors that underscore the central role of privacy in shaping these phases.

Firstly, during data acquisition, sensitive information about individuals is collected, thus requiring meticulous safeguards to prevent unauthorized access or misuse. Secondly, in the state inference phase, the amalgamation of data streams can yield nuanced insights into users' behaviors and actions, heightening the sensitivity of privacy preservation.

While the actuation phase is undoubtedly vital in a closed-loop approach, its prime emphasis lies on translating inferred states into actions rather than on the preservation of personal information. The real-time nature and immediate effects of actions in this phase pose a different set of challenges. However, the privacy considerations in the actuation phase are distinctly intertwined with

the outcomes of the preceding phases, as well as the executed actions themselves.

In this sense, the next sections of this chapter will provide an approach to privacy-preservation oriented toward the data acquisition and state inference phases of HiTLCPSs.

3.2 An approach to Privacy-Preservation in the Data Acquisition Stage

Even though HiTLCPSs can positively contribute to its users, we should not overlook the fact that the amount of data that these modern implementations are collecting to gauge skills and behavioral parameters, has increased significantly. IoT devices and mobile phones are currently responsible for the generation of large amounts of data, often becoming a source of highly sensitive information. This poses a challenge as accessing and sharing data often conflicts with widely accepted privacy policies and ethical principles. While certain privacy and security mechanisms aim to protect the sensitivity of datasets through anonymization processes, the risk of compromising users' privacy remains inherent.

Addressing this challenge in a HiTLCPS is possible through the adoption of a Human-Centric Security and Privacy approach [Ra et al., 2021]. It involves designing and implementing mechanisms that empower users to have control over their data and make informed decisions about its collection and usage [Nepal et al., 2022]. By incorporating user consent, transparency, and granular data access controls, this human-centric vision can help mitigate the risk of compromising users' privacy while still allowing for data-driven applications and services.

An important insight can be highlighted from the revision conducted in Chapter 2 regarding current privacy-preserving models and frameworks. Generally, the state-of-the-art contributions do not encompass the features of a Human-Centric Security and Privacy approach. Therefore, there remains a need for a solution that aims to integrate all or at least the majority of these characteristics. In this context, one of the significant contributions of this research is the proposal of a framework that enables privacy-aware data acquisition and privacy-preserving data sharing within the scope of the HiTLCPS concept.

3.2.1 PACHA: A Privacy-Aware Component for a HiTL-IoT Approach

The Privacy-Aware Component for a Human-in-the-Loop IoT Approach (PACHA) is our proposed framework that defines a mediation model for privacy-aware IoT data acquisition and privacy-preserving data sharing in a HiTL environment between Data Owners (DOs) and DRs. On one side, the DO is the individual or end-user who manages a set of IoT resources that produce data either passively or through interaction, and on the other side, the DR is the entity that seeks access to that data.

The two main components that make up the architecture of this proposed framework are the PACHA Privacy Orchestrator (PPO) and the PACHA Privacy Interagent (PPI), as depicted in Figure 3.2.

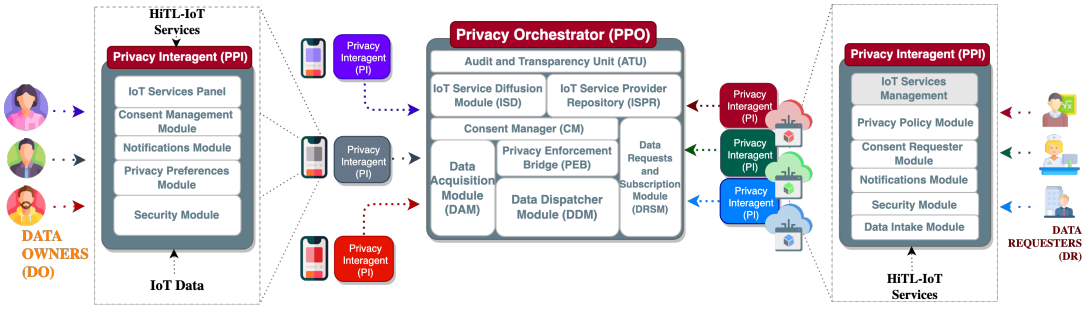


Figure 3.2: PACHA: The Privacy-Aware Component for a Human-in-the-Loop IoT Approach Framework

The main functions of the PPO are twofold. Firstly, it serves to facilitate and moderate the exchanges between the DO and DR. Secondly, it securely retains the data related to the IoT resources that the DO has chosen to share in an encrypted manner. The PPO is based on a modular architecture, as shown in Figure 3.2. Each of these modules fulfills a specific function, which is detailed in Table 3.1.

On the other hand, the PPI is an instance on both the DO and the DR side. On the DO side, the PPI allows the DO to learn about the DRs, access their respective privacy policies, set privacy preferences, and manage their resource data-sharing profiles. When a DR fulfills the role of a service provider, the PPI also informs the DO about the nature of the offered services. In that case, the PPI on the DR side enables the IoT services management module in addition to the consent-requesting tasks, and the definition of privacy policies. Table 3.2 sums up these modules with their respective functionality in each of the entities.

3.2.2 Privacy-Preserving Model

To align with the PACHA framework, a privacy aware data acquisition implementation for HiTLCPSs must ensure that the elements responsible for data acquisition and interaction with the DO and DR embody the characteristics of the components. For the DO interagent, a device or a collection of personal devices could perform the necessary functions. Similarly, the technological infrastructure of the DR could instantiate the PPI. As for the PPO, it was initially designed to reside in an accessible resource, such as cloud infrastructure, that is available to both DS and DR.

However, the fact that an element such as the PPO is meant to be instantiated within a third-party centralized environment, such as a cloud server, implies a relationship of trust. Although the framework includes a module dedicated to transparency and auditing, the fact that all actions derived from the data-sharing events (e.g., consent requests and responses) are handled and recorded

Table 3.1: PACHA Privacy Orchestrator Modules and Functions

PACHA PRIVACY ORCHESTRATOR	
MODULE	**FUNCTION**
IoT Service Providers Repository (ISPR)	Gathers the information from each of the data consumers, including descriptions, privacy policies, and previous user evaluations. Provides DR with a query token to interact with the DRSM.
IoT Services Diffusion (ISD)	Dissemination of IoT services information including privacy policies, to keep users informed.
Consent Manager (CM)	Handles the permissions granted by the DO to DR. Includes a notification engine that interacts directly with the PPI. Communicates with DRSM to inform DR regarding any DO decision.
Privacy Enforcement Bridge (PEB)	On-the-fly rule generator that interacts with the CM and the DDM.
Audit and Transparency Unit (ATU)	The transparency module was devised as a compliance information portal for regulatory authorities.
Data Acquisition Module (DAM)	Responsible for the data acquisition procedures and registry for DO devices. Acts as a re-encryption point of the DO data
Data Dispatcher Module (DDM)	Holds the values of the IoT Resource data attribute. Creates the subscriptions for DRs, based on the PEB rules.
Data Requests and Subscription Module (DRSM)	Manages all queries, requests, and responses. In the case of a consent request, this entity routes it to the CM.

by a centralized entity undermines their traceability. These problems could exacerbate in the case of a compromised server.

To cope with these issues in this section we present a privacy-preserving model that leverages the intrinsic features of the blockchain technology for consent management and transparency in Human-Centered IoT environment. Its architecture is depicted in Figure 3.3.

This novel proposal leverage the conceptual features of PACHA, by providing a transparent data sharing and consent management for all participants in the system, and by leveraging the features of blockchain. The components and participants of this model are described below.

Data Owner: DO hold the title of the IoT resources that generate the data within their domain. From the point of view of the privacy-preserving model,

Table 3.2: PACHA Privacy Interagent Modules and Functions

PACHA PRIVACY INTERAGENT		
ENTITY	**MODULE**	**FUNCTION**
DO	IoT Services Panel	Allows the DO to explore the registered and suitable IoT Services. This module holds the services' details, the provider's id, and the privacy policy.
DR	IoT Services Management Module	Allows the DR with service-providing capabilities to manage its services.
DO	Consent Management Module	Through this module, the DO can establish and manage (grant, reject, or revoke) his/her consent.
DR	Consent Request Module	This module enables the DR to request consent to access the data from the IoT devices from the DO
DO/DR	Notification Module	This module oversees displaying incoming alerts issued by the PPO.
DO	Privacy Preferences Module	In this module, the DO can define his/her privacy preferences. Based on these definitions the IoT Service Panel highlights certain services over others
DR	Privacy Policy Module	This module allows the DR to define the privacy policy to handle the data flows
DO/DR	Security Module	This module carries out cryptographic tasks
DR	Data Intake Module	Through this module, the DR can access the data shared by the DOs either for internal processing or to provide a service.

the main tasks of DO are related to the management and consent control of IoT resources (grant, deny or revoke data access), with respect to the various DRs.

IoT Resources: These are physical or virtual manageable elements that generate IoT data. Examples of these resources are the sensors in a hand-held device or within a wearable, or those sensors attached to new domestic appliances. These elements can sense data from the environment and context.

IoT Gateway: The IoT Gateway funnels all the data produced by the IoT resources and enables actions to be taken by the DO within the data sharing and consent management process, including the management of resources. The IoT Gateway also acts as a blockchain node and holds an instance of the PPI.

Data Requester: This is the party interested in obtaining data from IoT resources for further processing. A DR can be a plain data consumer interested in receiving a single stream of sensed data or even an elaborate IoT service provider that combines a variety of sensed data. Among its main actions are the definition and registry of a privacy policy which includes data treatment details. Also, this participant is responsible for issuing consent and IoT data access requests.

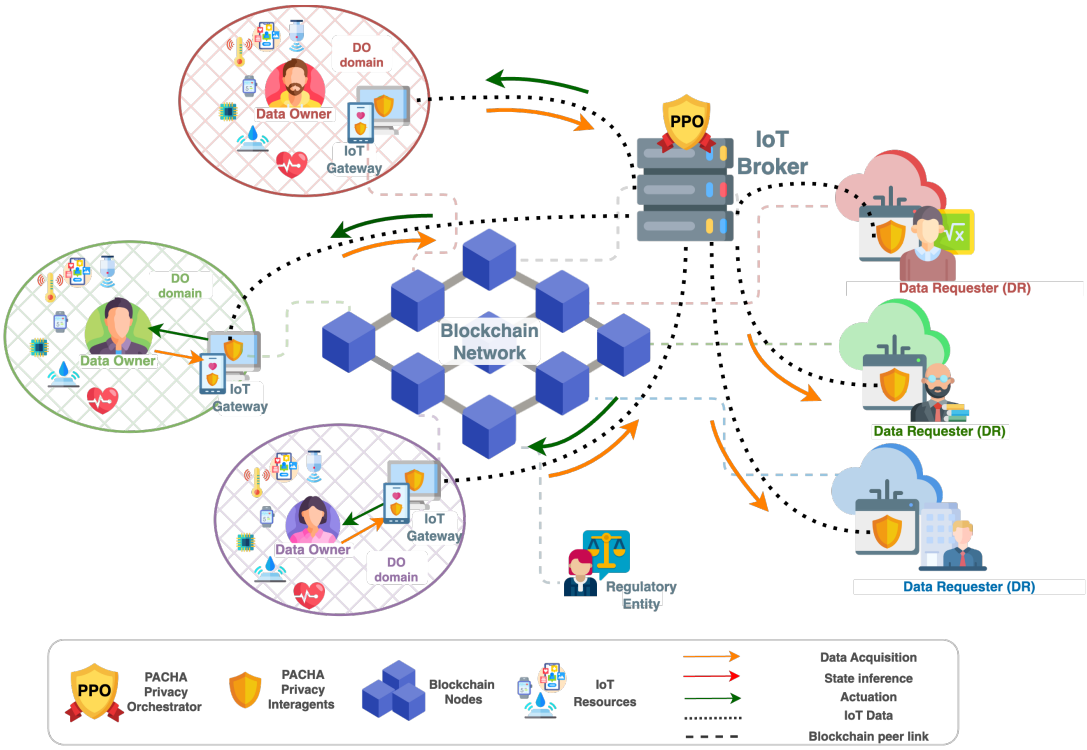


Figure 3.3: A Decentralized Privacy-Preserving Model for Consent Management, Data Sharing and Transparency between DOs and DR.

In the case that the DR is a services provider, the party must provide sufficient details regarding the service.

IoT Broker: This is an intermediary component that enables the interactions between IoT Gateways and DR devices. Its main actions are storing and safeguarding the data of the IoT resources shared by the DO, and retaining an internal DRs record, which includes, among other details, their privacy policy. This component implements a modified version of the PPO.

DR System: This is the component belonging to the DR through which all the actions of this participant are channeled. This component holds an instance of the PPI and acts as a blockchain node.

Blockchain Network (BN): This is a decentralized network made up of nodes or peers that hold an immutable ledger. This immutability feature ensures the integrity of every transaction generated by the nodes during the process. Each component in this model - IoT Broker, DR Device, and IoT Gateway - runs a node of the blockchain network, which allows them to keep a replica of the ledger and trigger transactions.

Regulatory Entity (RE): This is a passive entity in what concerns the resource management, consent, and data sharing process. Its role is to enforce the DR's privacy policies and supervise their compliance. The role of this entity is to audit DRs and IoT Brokers, as per the guidelines established by higher regulatory authorities (e.g., national data protection agencies). This entity also mediates between DOs and DRs, when a dispute arises. Likewise the rest of participants,

this entity is also part of the blockchain network.

3.2.3 Threat Model

It is important to emphasize that from the perspective of a DO, the IoT Broker, the DR Systems, and the RE are third party components with different trust relationships. In this sense, our threat model starts by assuming that the RE is a trusted party that oversees DR systems' actions and their behaviour. DRs could be initially considered as untrusted parties; nonetheless, they must be approved by the RE before joining the network. Only endorsed DR can register into the IoT Brokers, instantiate the PPI with their system along with the blockchain node, and carry out the consent and data release process. Therefore, for this threat model we assume that IoT Brokers and DRs are semi-trusted party, which honestly follow the overall consent and data release process but could be interested in learning any additional information derived from the procedures. This honest-but-curious nature could drive these two entities into performing misbehaved activities and/or even attacks, turning them into malicious parties.

For instance, a malicious IoT Broker would be tempted to collect the data, to further use it without the owners' consent leveraging the fact that this entity is in charge of temporarily storing the data from the registered DOs' IoT resources.

Regarding the DRs, although they are certified by the RE, this fact does not guarantee that any of them will not carry out a malicious action. For instance, a DR - acting as an adversary - would intend to gain access to as many IoT resources' data as possible, even the non-consented ones, generating many data access requests to saturate the IoT Broker, or generate several consent request to overwhelm the DO with new notifications.

The series of actions proposed in the next subsection comprise the consent and data release process. The design of this process considers the components and the actions of participants of the model along with the threat model, attack assumptions, and attacker capabilities.

3.2.4 Consent and Data Release Process

By the time the privacy orchestrator and the interagents have been instantiated within the corresponding components, the participants can register themselves and the consent-based data sharing process can initiate. At this point, it is assumed that during the registration process, the orchestrator and its agents have been issued with asymmetric cryptographic key pairs (public and private). Generated public keys are distributed among all components.

To ease the description, the consent and data release process has been divided into five phases, namely IoT Resources Provision, Consent Request, Consent Response, Data Release, and Consent Revocation. These are outlined below.

3.2.4.1 IoT Resources Provision Phase

IoT Resources Provision is the first phase of the process and is illustrated in Figure 3.4. It begins with the interaction between the DO and the IoT Gateway, by selecting the IoT resources to be shared. Once the choice is done, the PPI in the IoT Gateway generates the list of shareable resources (R) and requests its blockchain node to invoke the Smart Contract (SC) to update the ledger. This list includes some features of each shareable IoT Resource, namely its identifier, its type, and its data acquisition-frequency. When the resource registration transaction (TX) is generated and properly stored in the blockchain, the transaction identifier (TX_{id}) is sent back to the IoT Gateway, and it is encapsulated into a message by the PPI. This message (M_1) is signed with the private key of the DO (DO_{pri}) and forwarded to the IoT Broker. The PPO checks the provenance of the message, pulls the TX_{id}, and requests its peer in the BN to fetch R. Once the list of resources is retrieved, the PPO allocates resources to store the IoT resource data that will be transmitted from the IoT Gateway. When the infrastructure is in place, the PPO notifies the PPI in the IoT Gateway to start sending the resource data. These data before leaving the IoT Gateway is encrypted with the public key of the DO (DO_{pub}) to preserve their confidentiality in front of the IoT Broker. At the same time, the PPO informs the registered DR agent, that a new set of IoT resources is available.

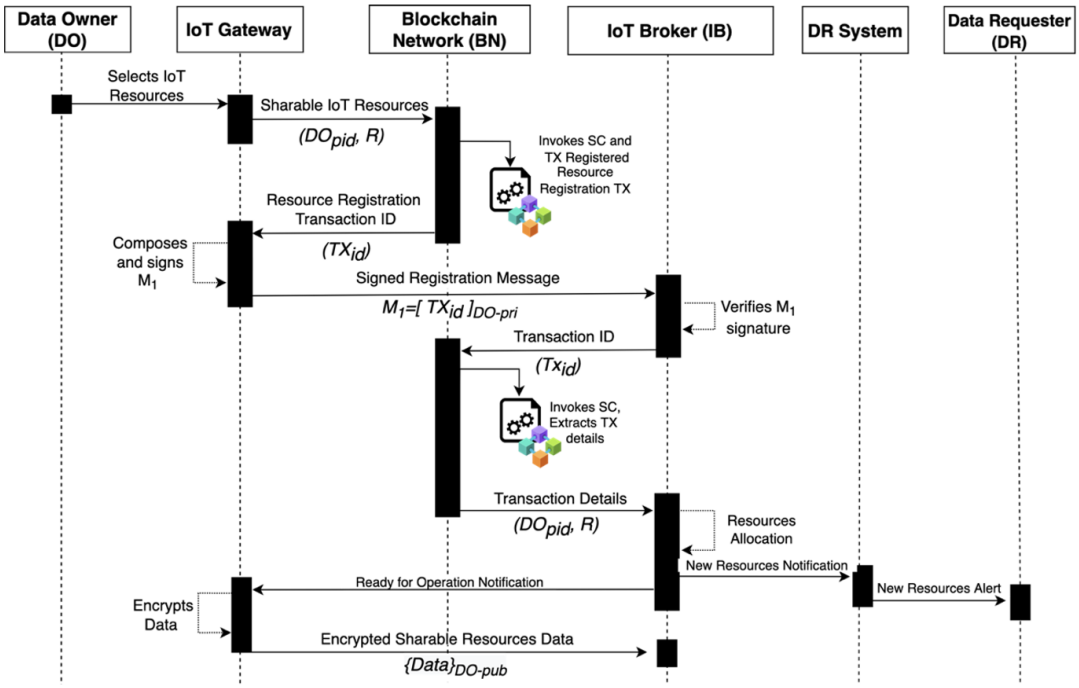


Figure 3.4: Sequence Diagram to illustrate the IoT Resources Provision Phase

3.2.4.2 Consent Request Phase

To gain access to the data of the IoT resources, the DR must issue consent requests via its PPI, which periodically fetches the list of shareable resources from the ledger. Each consent request is formed by the identifiers of the resources

(R') whose data is intended to be acquire by the DR. For instance, let us suppose a particular DR would like to access the data from three IoT resources managed by DO_1, one resource from DO_2 and two resources from DO_3. In this assumption, the DR device would generate six consent requests regardless of the type of IoT resource; in other words, the DR can select the same or different types of resources from the available pool. Each request is handled separately and, by invoking the SC, a series of transactions is generated. The PPI in the DR system sends to the IoT Broker these transactions' identifiers (TXs_{id}) embedded in a message (M_2) signed with the DR private key (DR_{pri}). The PPO verifies the provenance of the message and extracts the TXs_{id}, which will be later used by its peer. The transaction details are retrieved by querying the ledger after invoking the SC. The IoT Broker receives R' and, from its internal registry, generates consent request messages (M_3) addressed to each of the respective DOs. In the case of the previous hypothetical scenario, the IoT Broker would generate three consent request messages, one for each of the DO.

The consent messages are signed by the IoT Broker and include the DR privacy policy (DR_{PP}) endorsed by the RE, the DR public key(DR_{pub}), and TXs_{id}. Figure 3.5 represents this phase as a sequence diagram.

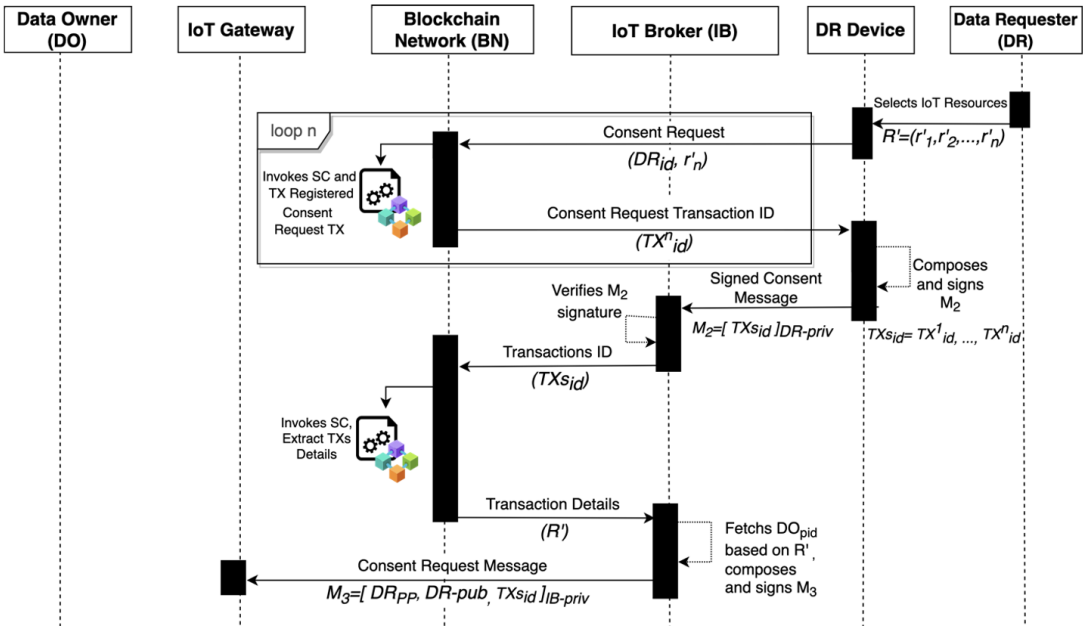


Figure 3.5: Sequence Diagram to illustrate the Consent Request Phase

3.2.4.3 Consent Response Phase

Once M_3 is received, the IoT Gateway checks its provenance and requests its BN node to extract the details of the transaction(s). With the list of requested IoT resources (R') and DR_{PP}, the DO can take one of the following decisions: i) grant full consent (authorize the accessing and the processing of all requested resource data); ii) grant partial consent (some of the requested resources are approved for accessing and processing); iii) deny the request (accessing and processing of the requested resources is not allowed). The decision taken by

the user is expressed through its PPI. In case there is at least partial consent, the IoT Gateway generates a consent state matrix structured by the list of approved resources, their ID, its consent state (granted/rejected), and the period of validity (in the case of granted resources). This structure is later registered within the blockchain as a new transaction. Meanwhile, the PPI generates the re-encryption key (rek) based on its private key and the public key of the requesting DR. The transaction ID and the re-encryption key are forwarded to the IoT Broker in a message (M_4) signed by the IoT Gateway-PPI. The PPO checks the provenance of the message and requests its node to invoke the SC to pull the content of the transaction. The PPO caches the re-encryption key during the consent validity, updates its inner registry according to the new consent state of the registered resources, and produces a notification message to the PPI of the DR informing the DO's response. The re-encryption key is stored by the PPO during the consent validity Figure 3.6 depicts this process. In this phase, the PPO keeps permanently updated its inner registry, and since each DO has its specific fields on it, the IoT Broker is capable of handling consent responses from multiple DO.

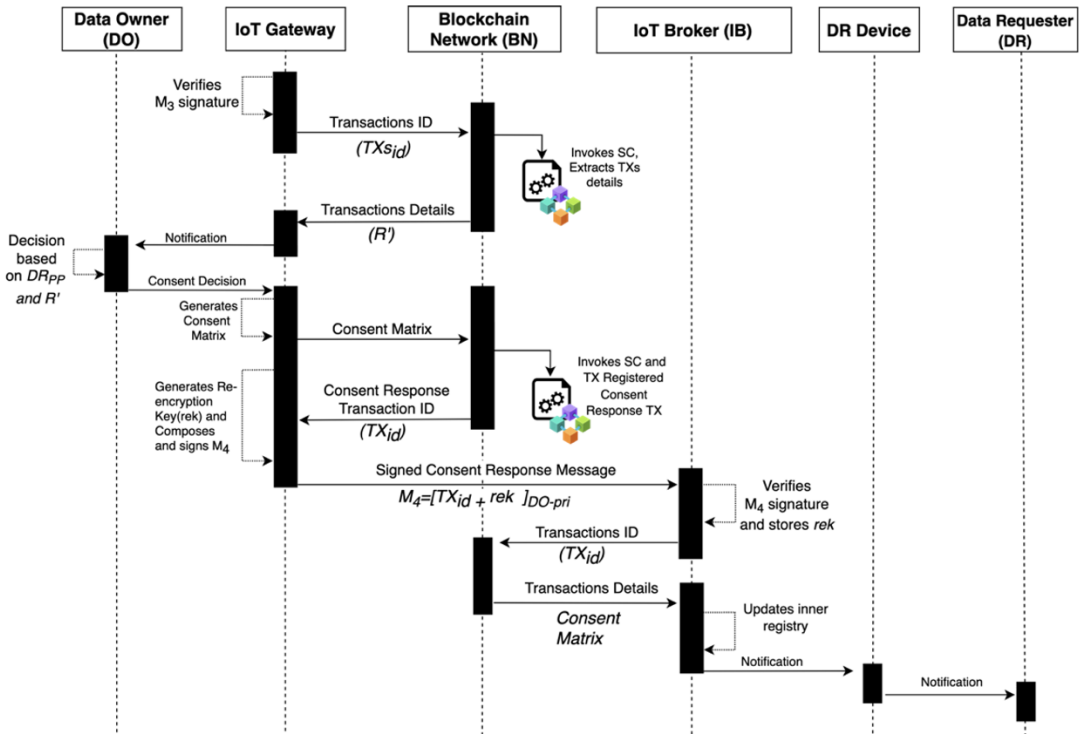


Figure 3.6: Sequence Diagram to illustrate the Consent Response Phase

3.2.4.4 Data Release Phase

From the moment the DR's PPI receives the consent granting notification, this participant can retrieve data from the IoT Broker through its agent during the period of validity of the consent. The DR selects the granted IoT resources from which he/she wants to retrieve data (R'') and issues a data access request that transacts in the BN. The ID of this transaction (TX_{id}) is forward from the DR device to the IoT as a signed data access request message (M_5). The IoT Broker

verifies the message sender, and fetches the data access request by querying the SC. Once retrieved this request, this entity can update its inner registry by invoking the SC and compare the request with the updated registry. If the requested resources match the consent the updated registry, the IoT Broker re-encrypts the data with the re-encryption key generated by the DO in the previous phase. The data sharing event details are recorded into a transaction within the ledger. The TX_{id} is sent to the IoT Gateway in a message (M_6), signed by the IoT Broker using its private key (IB_{pri}), to keep the DO informed about the amount of data requested by the approved DR. On the DR side, the received resource data is decrypted by its PPI using the DR's private key. However, in the case the data request does not match with the inner registry, the IoT Broker increases his non-allowed requests counter. While the counter does not exceed an established threshold the IoT Broker notifies the DR that the request is invalid. Else, the DR is blocked and reported to the RE. Figure 3.7 presents this process as a sequence diagram.

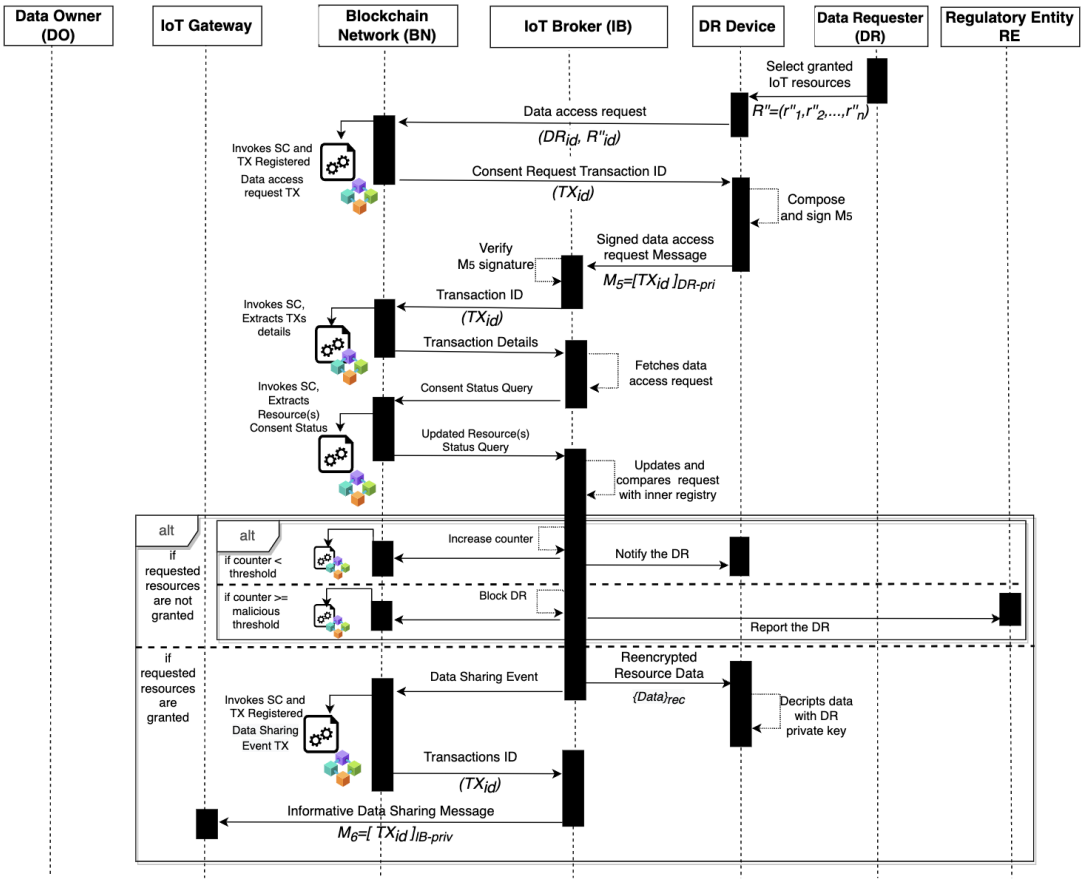


Figure 3.7: Sequence Diagram to illustrate the Data Release Phase.

3.2.4.5 Consent Revocation and Data Deletion Phase

Every consent issued by a DO has a set expiration date. Nevertheless, it may be revoked by the issuer before the end of its validity. The DO may revoke previously granted consents to one or more DRs through the PPI in the IoT Gateway. The revocation evidence is recorded within the ledger as a TX after

the IoT gateway node invokes the SC. The TX_{id} is forwarded to the IoT Broker in a signed message (M_7). The PPO verifies the origin of the message and delegates it to its blockchain node to invoke the SC to retrieve the transaction details. Based on the details that include the new version of the consent state matrix, the IoT Broker updates its internal registry and notifies the corresponding DR about the revocation. It is possible that within the consent revocation transaction, the DR may be asked to delete all previously obtained and processed data. In this case, after the notification, the DR must perform the data deletion processes and generate a transaction that will be stored within the ledger with the data deletion details. The ID of this transaction is embedded in a signed data deletion message (M_8) and sent to the RE, who is going to verify its origin and retrieve the details of the transaction by invoking the SC. These details will be used in the audit processes over the DR system. Figure 3.8 depicts this process in a sequence diagram.

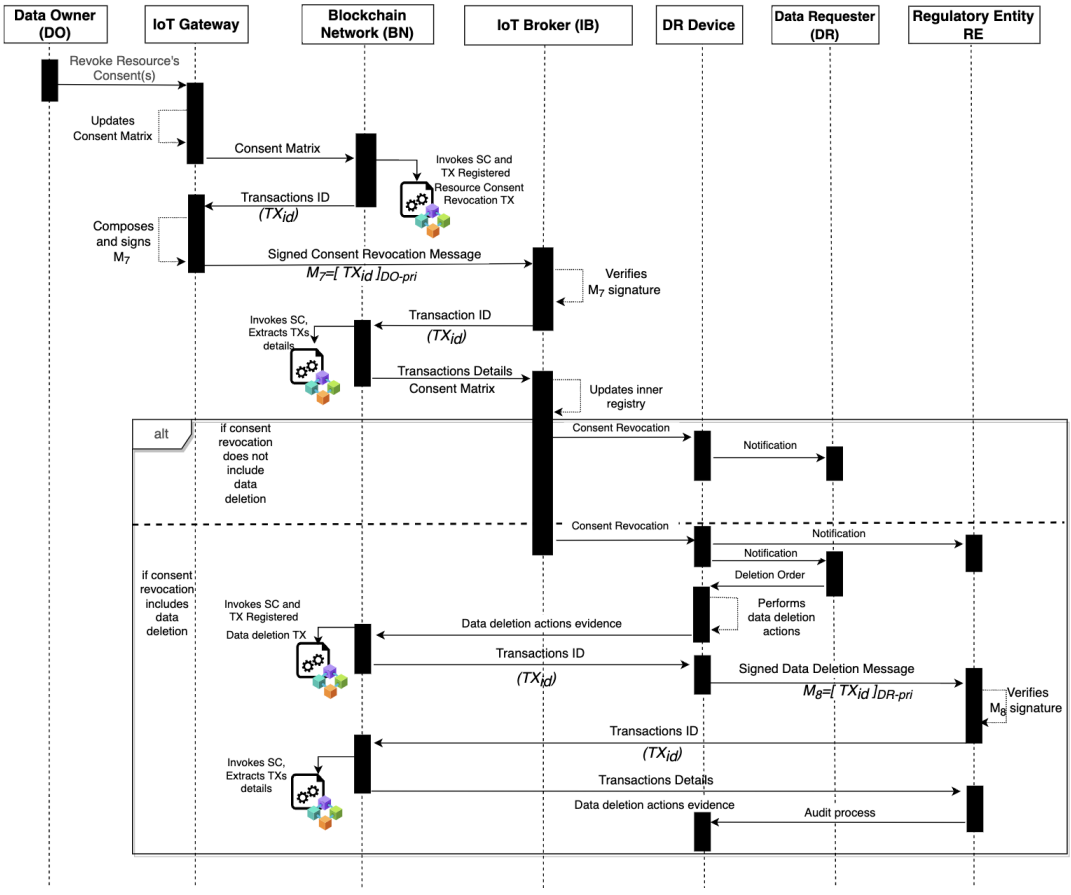


Figure 3.8: Consent Revocation and Data Deletion Phase as a sequence diagram.

To show the feasibility of this approach, the proposed model was implemented, deployed in a test environment, and assessed using a realistic scenario. The details of the implementation will be covered in Chapter 5, while its assessment will be addressed in Chapter 6.

3.3 An approach to Privacy-Preservation for the State Inference Stage

Current applications and services provided by HiTLCPSs still rely on a cloud-based AI approach, which means, that the data produced by the end-user devices is pushed to a third-party infrastructure, where the data inference is carried out through AI. Sending all this data over to an entity outside the user's scope involves not only additional privacy risks but also storage and communication challenges, especially those related to latency and bandwidth consumption.

To tackle some of these issues, new proposals that come out with novel manners of distributed processing are drawing attention and becoming increasingly relevant. One clear example is Edge AI, which is intended as an alternative to relocating the state inference processes closer to or at the data sources. Edge AI combines the capabilities of edge computing and artificial intelligence to provide systems where learning algorithms can be deployed at endpoints, including user devices. This allows, among other benefits, to reduce latency, and decrease bandwidth and cloud storage requirements, hence speeding up decision-making processes. However, since learning models to be deployed on edge devices require prior training on a centralized server, this could still lead to privacy concerns. Therefore, a distributed training approach on the edge would mitigate this issue. In this regard, FL has become the de facto paradigm for collaborative training in a network of devices. Its most salient feature is achieving distributed training, bypassing the need to move data to an external server managed by an untrusted third party [Khan et al., 2021; Nature, 2021].

3.3.1 Artificial Intelligence at the Edge

AI has established itself as one of the most disruptive technologies ever, and together with cloud computing has improved upon various processes from a variety of industries and businesses. The integration of AI with cloud computing delivers greater productivity, efficiency, and accuracy in the AI pipeline. It also allows the agile development of solutions tapping into the high data volume capacity that cloud environments offer.

Nonetheless, the high demand for services and applications based on this paradigm is generating storage and connectivity issues (latency and bandwidth consumption). Also, the uncontrollable collection and use of data increase the concerns of end users regarding the preservation of their privacy.

In this regard, a paradigm called Edge AI comes up with the idea that AI workflows should include the devices at the very edge of a network, standing in contrast to the notion of cloud-based AI where the pipeline runs entirely in a centralized entity. Edge computing supports Edge AI by bringing computation and storage closer to the point of request to decrease bandwidth consumption and deliver low latency. Edge AI enables learning algorithms to be deployed directly onboard end devices; hence, the processing stage is performed at the edge.

However, deploying Deep Learning (DL) models in constrained-edge-device environments is setting up new stakes. For instance, Bhardwaj et al. [2021] specify three main challenges namely, computation-aware learning on IoT, data-independent model compression from small-data, and communication-aware deployment of deep learning models on multiple IoT devices. The first challenge is related to the size of the learning model to be deployed into edge devices, and how to reduce it without affecting its accuracy. The second challenge lies in the lack of the original data sets to perform model compression. Finally, the last challenge encompasses the heavy communication at each layer of the deep network when a model is distributed among devices.

To these challenges, we can add that the large volume of data collected from the IoT environment may prevent big data analytics from performing quickly. Also, some approaches in the IoT context are limited to domains with low-dimensional sensory inputs [Wei et al., 2020].

Addressing these challenges would allow a large-scale adoption of intelligence at the IoT edge. This also would overcome most of the issues derived from cloud-based approaches; however, Edge AI still resorts to some extent to the cloud for training models before their deployment. Therefore, it is necessary to complement this edge approach with privacy-preserving mechanisms. In this regard, FL has emerged as a potential solution that eases collaborative learning without disclosing training data sets [Nguyen et al., 2021]. FL is a PET proposed by Google, where several entities collaborate in solving a learning problem orchestrated by a service provider or central server [Kairouz et al., 2021].

In a traditional learning approach, a group of n end-users $\{U_1, ..., U_n\}$ consolidate their data $\{D_1, ..., D_n\}$ into a new dataset $\mathcal{A} = D_1 \cup ... \cup D_n$ to train a learning model $\mathcal{M}_T$, achieving an accuracy $\mathcal{P}_T$. Whereas in FL, each data owner U_i, where $i \in [0, n]$, trains a model $\mathcal{M}_{FED}$ collaboratively, without disclosing its data D_i to the rest of the participants, ensuring that the accuracy of this model $\mathcal{P}_{FED}$ is close to $\mathcal{P}_T$. For a federated model is possible to determine its accuracy loss δ as follows:

$$|\mathcal{P}_{FED} - \mathcal{P}_T| < \delta \tag{3.1}$$

Only the train parameters of the federated clients' models return to the server for aggregation and the update of a global learning model. Finally, the new global model is sent back to the end-user devices. This approach represents a paradigm shift in the way models have learned until now.

FL is a collaborative learning approach with a promising application in several domains in which data cannot be directly aggregated for training learning models due to data security, privacy protection, or intellectual property rights [Yang et al., 2019]. Its intrinsic privacy preserving characteristic makes it a suitable candidate for the HiTLCPS state inference tasks.

Nevertheless, despite FL's great potential, some critical research challenges must be overcome. For instance, according to Zhao et al. [2018], non - Independent

and Identically Distributed (IID) local data can directly impact FL models by reducing their performance. Bonawitz et al. [2019] even claim that FL workflow requires a model that needs human intervention. Moreover, node selection and heterogeneity, communication, and synchronizing issues are contributing to the slow convergence rate and therefore must be properly addressed. Additionally, training overheads impose several restrictions, mainly with huge data volumes produced in IoT environments.

3.3.2 State inference in the IoT Gateway

The privacy-preserving model presented in section 3.2.2 comprises various components and defines a set of interactions to provide DOs with a way to manage their IoT resources and conduct a secure data-sharing process following a consent-based access control approach. Moreover, this approach aims to make transparent the intents and actions from the involved entities regarding IoT data access.

While up to this point, the model contributes with a privacy-aware data acquisition phase for HiTLCPS, privacy issues at the inference phase level remain latent. Currently, this type of implementation performs data processing on an infrastructure belonging to the HiTLCPS service provider. These actions result in inferences that may disclose sensitive aspects of DO, leading to additional privacy concerns and ultimately affecting the adoption of these systems.

In this regard, to minimize third-parties data collection, there is a growing trend to move the processing tasks closer to the edge. This action would allow to better preserve DO privacy and at the same time tap into the unused processing power of some edge devices. Given this premise, in this section, we introduce our approach by extending our previous proposal described in section 3.2.2 and combining it with a suitable approach based on FL to carry out the state inference phase at the IoT Gateway level.

For a state inference at the IoT Gateways level, the IoT Broker, in addition to implementing the Privacy Orchestrator functions, must furnish service providers with the necessary resources to instantiate the HiTLCPS service. After service instantiation, this component will act as a central aggregation server to manage learning models and coordinate the collaborative learning mechanism with the associated IoT Gateways. This implies that each IoT Gateway subscribed to that service, contains a local version of a learning model trained with the data from its associated IoT Resources. The trained models are periodically sent to the IoT Broker for its aggregation and the generation of a global version of the learning model, which will be redistributed among the federated clients. In this manner, HiTLCPS services can be offered within each personal domain without the need for the data produced by the IoT Resources to leave the DO premise.

This approach is represented in Figure 3.9 and explained through a use case in which two service providers interact with DO through an IoT Broker. In this case, the first service provider maintains the inference process on its side, whereas

the second service provider instantiates the service in the IoT Broker. All DOs are subscribed to the second provider's service, and only one is subscribed to both. As can be seen in the graph, only the IoT data from the last DO are sent to the IoT Broker to access the service furnished by the first provider. In the case of the second service, all DOs collaborate in the training process and share their learning models with the IoT Broker, before receiving back the aggregated model. Once the final model is available, inferences can be performed locally. Although in both cases, the second phase of the HiTLCPS concept is fulfilled, an important aspect to be evaluated is the accuracy of these inferences.

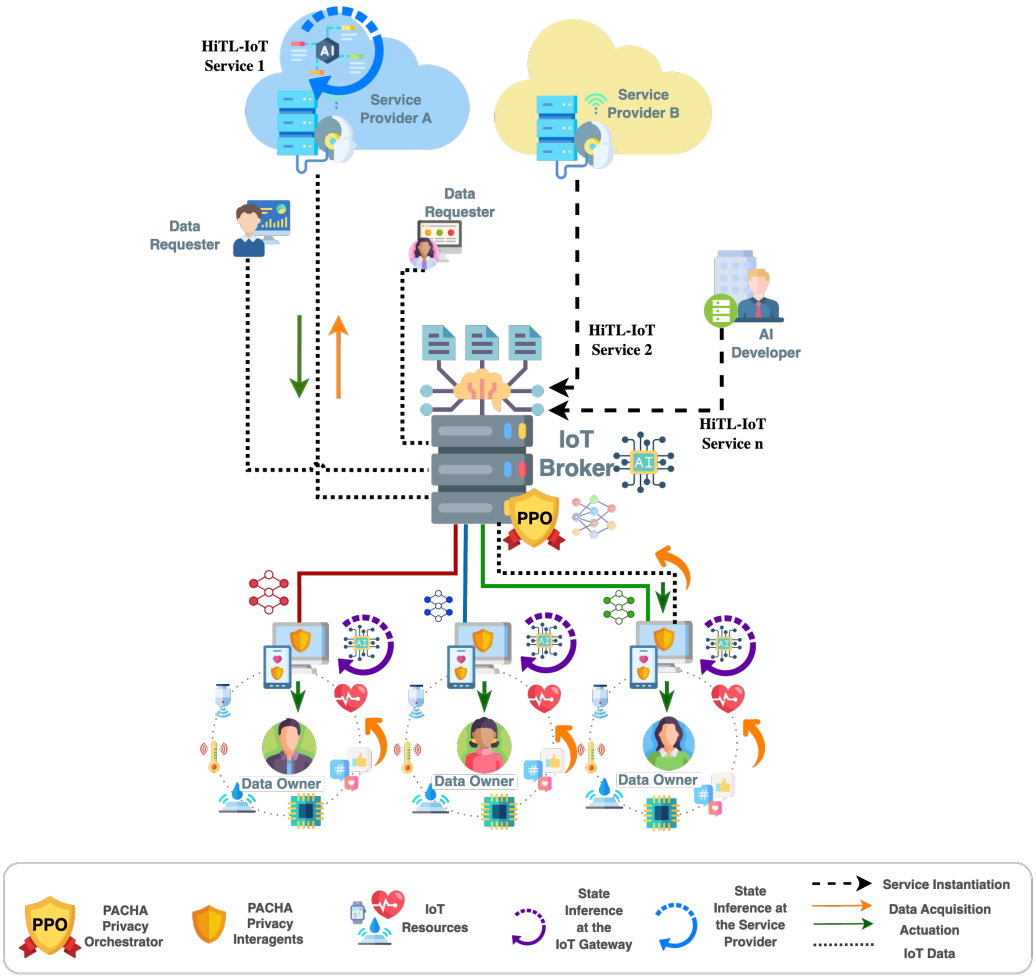


Figure 3.9: Extending the privacy preserving model with state inference in the IoT Gateway

Similar to the previous approach, the details of this implementation and assessment are cover in Chapter 5 and Chapter 6 respectively.

3.3.3 State Inference through IoT Resources

Apart from proposing an approach that considers the IoT Gateway as an element capable of performing state inference and based on a theoretical perspective, this

section provides a roadmap for a future iteration of this approach in which this task can be delegated to and performed by the IoT resources from the DO domain.

A common feature among these components is their constrained hardware in terms of memory and computation. Therefore, to execute HiTLCPS state inference through these devices, it is necessary to tackle the three major challenges pinpointed in Section 3.3.1 namely computation-aware learning on IoT, data-independent model compression for learning from small data, and communication-aware deployment of deep learning models on multiple IoT devices.

The first challenge could be addressed by using a compression model to make deep learning algorithms more suitable for edge devices [Hinton et al., 2015; Han et al., 2015]. In our model, the IoT Gateway would adapt AI models to reduce both computation and communication costs without affecting accuracy in IoT devices. For that, the IoT Gateway should use Pruning to remove redundant or useless weights or even channels; Quantization, to reduce the number of bits used for representing weights and activations; and Knowledge Distillation (KD) to train a significantly smaller student network to mimic a large one, based on the compressed IoT Gateway's teacher model. This latter technique would allow us to directly reduce the number of layers compared to the teacher model [Bhardwaj et al., 2020].

The second challenge could be tackled using Dream Distillation [Bhardwaj et al., 2019b], a KD-based technique that does not rely on access to any real data. It compresses a deep learning network without using the original training set or any alternate real data while achieving comparable accuracy. It uses metadata and the previous teacher network to generate a new dataset of synthetic data, that can effectively distill relevant knowledge from the teacher to the student without using raw data.

For the third challenge, this new approach would consider Networks of Neural Networks (NoNN) [Bhardwaj et al., 2019a], a highly-efficient compressed deep learning paradigm for inference on resource-constrained devices. Training an individual student to mimic a specific partition of the teacher's knowledge is significantly easier than mimicking the teacher's entire knowledge. NoNN achieves higher accuracy with minimal communication overhead among the students. Parallelizing the student architecture model results in significantly lower memory, computations, and communication. The individual student models do not communicate with each other until the final fully connected layer.

The use of Edge AI at the IoT resource level does not incur privacy issues, since the deep learning models to be deployed are previously trained by the IoT Gateway, which is a fully manageable element controlled by the DO. Moreover, the HiTL approach is also considered in the outcome of the processing stage by including reinforcement learning capabilities to fine-tune predictive learning models. By considering these approaches, the vision of a model that allows other kinds of state inference processes and the deployment of services in different contexts becomes feasible.

3.4 Privacy-preserving HiTLCPS integration

HiTLCPS are designed to operate within a specific context. However, in larger environments such as smart cities, the objective is to integrate these systems to enable interoperability. In terms of services, it is possible for one or more services to be shared across multiple systems. Additionally, from the DO perspective, a user registered in one system may also be associated with other ones.

Considering the proposed privacy preserving approaches, Figure 3.10 sketches a scenario in which coexists diverse HiTLCPSs environments and at the same time integrate different the data acquisition and state-inference approaches presented previously. In this figure, three IoT Brokers can be observed, representing three different domains, a group of DOs, and a set of DRs, including service providers. In this model representation, it can also be seen for instance, that DO III, DR II, and service provider III are associated with more than one IoT Broker simultaneously.

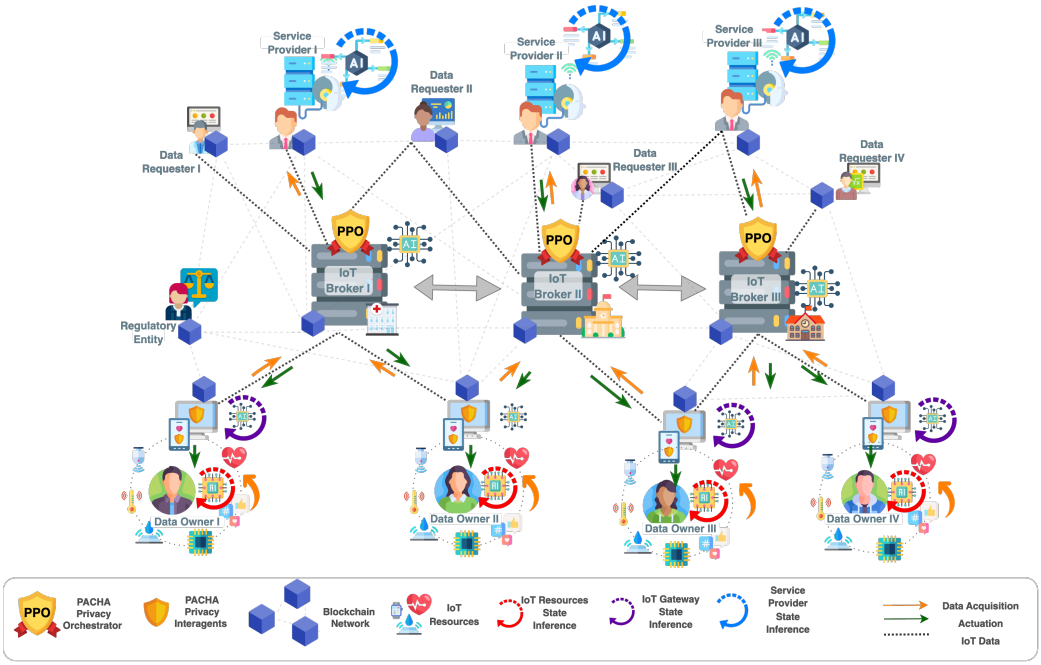


Figure 3.10: A HiTLCPS environment with different state inference approaches and integrating diverse contexts.

In the case of interoperable systems, all settings related to preferences and privacy policies can be set only once, which would contribute to the seamless interaction between both DOs and DRs. In addition, this integration can be considered beneficial, especially for improving the processes related to state inference at the IoT Gateway level. By having channels linking several IoT Brokers, Federated Transfer Learning techniques [Chen et al., 2020] could be used to transfer learning models previously trained in one environment to improve the performance of a model trained on a different dataset.

This conceptualization serves as the preamble to the proposed integration model, which will be addressed in the next chapter of this thesis.

3.5 Summary

With the proliferation and widespread adoption of personal IoT devices, the original concept of IoT has evolved, giving rise to new paradigms such as HiTLCPSs. While these implementations offer numerous benefits and positive influences on individuals, their pervasive nature raises significant privacy concerns, particularly regarding data acquisition and processing.

This chapter introduced the notion behind HiTLCPSs, highlighting the data acquisition and state inference phase. It then explores approaches toward a privacy-preserving model for HiTLCPSs. The proposed model incorporates a human-centric mechanism for control, leveraging our proposed PACHA framework, making data acquisition and sharing tasks transparent with a state inference process supported by AI in the edge.

Finally, this chapter lays the groundwork for a model that integrates diverse privacy-preserving HiTLCPSs from different contexts. The forthcoming chapter of the thesis will delve deeper into the development of a proposal aligned with this idea.

Publications based on this chapter's work

- Rivadeneira, J. E., Sá Silva, J., Colomo-Palacios, R., Rodrigues, A., Fernandes, J. M., and Boavida, F. (2021). A privacy-aware framework integration into a human-in-the-loop iot system. In *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 1–6;
- Rivadeneira, J. E., Jiménez, M. B., Marculescu, R., Rodrigues, A., Boavida, F., and Sá Silva, J. (2023b). A blockchain-based privacy-preserving model for consent and transparency in human-centered internet of things. In *Proceedings of the 8th ACM/IEEE Conference on Internet of Things Design and Implementation*, IoTDI '23, page 301–314, New York, NY, USA. Association for Computing Machinery;
- Rivadeneira, J. E., Borges, G. A., Rodrigues, A., Boavida, F., and Silva, J. S. (2023a). A unified privacy preserving model with ai at the edge for human-in-the-loop cyber-physical systems. *Submitted to Internet of Things; Engineering Cyber Physical Human Systems* **(Q1)**;

Chapter 4

An Integration Model for Privacy-Preserving HiTLCPS Toward Sustainability in a Smart City

Contents

In close alignment with the groundwork laid in the previous chapter, which introduced the concept of HiTLCPSs and provided a model toward privacy preservation particularly emphasizing the phases of data acquisition and state inference, this current chapter extends to the integration of these systems within the larger context of Sustainable Smart Cities (SSC).

Nowadays SSC are gaining momentum, supporting a wide variety of applications and solutions to not only improve citizens' quality of life but also the efficiency of urban services while meeting the economic, social, cultural, and environmental needs of present and future generations. To provide sustainability, smart cities are deploying cutting-edge IoT solutions based on on-the-fly data sensing and tapping into the proliferation of new urban and personal devices.

Currently, an increasing number of IoT-based proposals have targeted sustainability in smart cities. Unfortunately, these solutions, in addition to their heterogeneous nature, are primarily proprietary implementations that do not interact outside their scope and range [Brutti et al., 2019]. Thus, to integrate these solutions from various domains and truly provide efficient and effective services for stakeholders, one of the main challenges in tackling this multilayer complex system is interoperability [Tsampoulatidis et al., 2022].

The European Interoperability Framework for Smart Cities and Communities (EIF4SCC) [Commission et al., 2021] sets out a group of principles and recommendations for the improvement of service delivery at local, national, and EU levels. Among the principles on which this proposal and its recommendations are based are the human-centered approach, the protection of individual privacy, the guarantees of transparency and security among stakeholders, a participatory approach, data portability, and the implementation of seamless solutions based on advanced technologies (e.g., IoT, blockchain, AI, etc.).

In this chapter, our aim is to align with these principles and recommendations to propose a model that serves as a reference for the development, implementation, and integration of novel privacy-preserving HiTLCPSs, by leveraging the features of decentralized technology, such as blockchain. The objective of this integration model is to contribute to urban sustainability and foster interoperability among the various technological components of stakeholders in a smart city.

4.1 Background and Related Work

Before delving into the integration model's details, this section will provide definitions, review the background, and explore related work on this topic.

4.1.1 Interoperability

One of the features regarding the model is to enable the interoperability of smart city initiatives. NIST extends the IEEE definition of interoperability as *"the capability of two or more networks, systems, devices, applications, or components to work together, and to exchange and readily use information — securely, effectively, and with little or no inconvenience to the user"* [Gopstein et al., 2021].

In the context of this topic, several authors have proposed interoperability models focused on user data within the dynamics of smart cities. For example, Rahman et al. [2022] propose a hierarchical blockchain-based platform to ensure the integrity of IoT data and blockchain interoperability in smart cities. Their platform enhances confidence in managing citizens' information by guaranteeing the integrity of IoT data and traceability of operations. The authors address the complexity of heterogeneity within city organizations through a structured 'blockchain of blockchains' approach, creating a trustworthy platform for secure data communication. However, it is important to note that the number of layers in the hierarchical model of the blockchain of blockchains can affect latency, execution time, and validated transactions.

Kundu [2019] explores the crucial aspect of trust within a smart city, discussing use cases and examples of trust consensus in citizen dynamics. The paper also examines how blockchain and smart contracts can establish trust in data sanctity, verifiability, interoperability, and institutionalization. It presents examples categorized across four key areas relevant to smart cities: the impact of network effects on trust in governments and industries, strengthening the economy through trusted transactions, the concept of a liquid economy, and the exchangeability and interoperability of economies. The article further analyzes the significance of blockchain in gamification and reward systems for smart city ecosystems, emphasizing the role of trust in fostering closer and more secure economies among citizens. Lastly, the article explores the importance of blockchain in the governmental dynamics of smart cities, highlighting how implementing these technologies at the governmental regulatory level could contribute to the development of smarter and more trustworthy cities.

Brutti et al. [2019] propose a methodology and a modular, scalable, and multilayered ICT platform to tackle the challenge of cross-domain interoperability in Smart City applications. The paper addresses the secure, effective, and transparent exchange of information between systems with minimal inconvenience to users and active elements within smart cities. The platform, employing a modular non-blockchain approach, enables the integration of registry managers, urban data, business data, ontology data, authentication, and national or governmental services. By offering a horizontal platform, it facilitates the connection of diverse urban services while also enabling the provision of vertical services tailored to specific application contexts. This transparent information sharing between services benefits citizens within their respective contexts. While these services greatly contribute to interoperability among smart city systems, they must inherently instill trust and address privacy concerns, which could be achieved

through the implementation of blockchain systems.

Kusumastuti et al. [2022] conducted an empirical evidence study in Indonesia to analyze the influence of seeking and sharing data on these platforms. This paper focuses on how such behavior affects citizens' intention to share data that can be utilized in various domains and platforms beyond their own city. The study also presents a model that examines the positive or negative impact of users sharing data when smart city initiatives need to be aligned across different cities in the country. The model analyzes the influence of platform attributes, user attitudes toward the initiatives, perceived knowledge, social factors, user experience, and perceived user privacy. The authors conclude that smart city initiatives with greater interaction and the provision of useful information can influence usage and interest in data sharing, even if the initiatives originate from cities other than where the users reside

4.1.2 Privacy Preservation

In addition to ensuring interoperability, models must also prioritize the privacy of users and their data to increase human participation in HiTLCPS. For instance, Makhdoom et al. [2020] present 'PrivySharing,' an innovative blockchain-based framework designed for secure and privacy-preserving IoT data sharing within a smart city environment. The framework introduces a data preservation innovation based on the division of blockchain channels, where each channel is assigned a limited number of organizations responsible for processing specific data categories within the context of smart cities, such as health, mobility, energy, or finance. Furthermore, organizations can access user data through a regulated and embedded access control process facilitated by smart contracts, ensuring compliance with EU regulations, including GDPR data protection. However, the authors acknowledge the need for the implementation of a system that securely integrates IoT devices into the BN.

Kumar et al. [2021] present a Privacy-Preserving and Secure Framework (PPSF) for IoT-driven smart cities. This framework primarily focuses on two key features: a privacy scheme and an intrusion detection scheme. The privacy scheme is built on blockchain technology, while the intrusion detection scheme utilizes a module called Gradient Boosting Anomaly Detector (GBAD). The framework is motivated by the preservation and confidentiality of authorized citizen data, along with alerts for unauthorized users attempting to access the network. While this framework is specifically designed for IoT-driven data, it has yet to be tested in prototypes that can be deployed in real-world city environments. The authors plan to conduct future work to validate the framework through prototypes that can be utilized by citizens.

Some works approach privacy preservation from different fields but with something in common, which allows combining fields of action where the combined interaction generates privacy concerns. For example, in Xu et al. [2023], a privacy-preserving distributed optimization algorithm is established. Also, it is considered a multi-agents-based distributed convex optimization problem, where the objective functions can be non-smooth. Additionally, Qi et al. [2022]

discuss the potential of combining blockchain with the Internet of Healthcare Things (IoHT) concept, focused mainly on the privacy preservation of these systems. This survey addresses the care and protection of data leakage in medical systems and the risk that this may cause to patients. Therefore, this review aims to improve the reliability and privacy of the systems based on a blockchain approach and distributed ledgers. In Wang et al. [2019b], privacy preservation is evaluated in the challenges of social vehicular networks, taking into account the potential risks encouraged by the interaction of passengers in the natural dynamics of the network. The diversity of participants moving from vehicular to social vehicular networks requires a solution that mitigates security risks and personal data protection. Finally, Liu et al. [2021] address the privacy concerns in cross-organizational process workflows. These processes involve multiple organizations that commonly require collaborative tasks. Therefore, the paper proposes a correctness verification approach for cross-organizational workflows with task synchronization patterns. The approach ensures globally correct execution by leveraging the local correctness of each sub-organizational workflow process.

4.1.3 Solutions based on contemporary technologies

This review also considers the integration of advanced technologies such as IoT-based systems with Blockchain. IoT services play a significant role in driving smart features in cities, and the adoption of these systems can be influenced by the trust that blockchain provides in safeguarding citizens' data transactions. Khang et al. [2022b] present the concepts, methodologies, and solutions involved in designing infrastructure for smart city ecosystems. Their paper explores how IoT applications drive smart city systems and how they can be integrated with advanced data management and artificial intelligence technologies. The importance of monitoring systems over long-distance networks, such as LoRaWAN, and the need for trust systems for the monitored data, such as blockchain, are contextualized. Additionally, Khang et al. [2022a] delve into the updated frameworks for modeling, procuring, and building systems for smart cities by integrating blockchain and IoT technologies in greater detail. However, they also acknowledge the need to address privacy and interoperability challenges that arise from combining LoRaWAN and blockchain within the same context.

In addition to integrating network technologies with blockchain, it is crucial to explore the integration of IoT-embedded devices into this technology. Arnaudo et al. [2023] present a lightweight transaction protocol that facilitates the interaction and integration of embedded devices in blockchains using the LoRaWAN protocol. This protocol enables securely authenticated devices to integrate IoT devices despite the limited resources of embedded systems. It aims to reduce the amount of metadata transmitted by IoT devices and optimize the power consumption of embedded devices in blockchain systems. However, it is important to consider aspects such as latency and communication errors associated with LoRaWAN in these models.

4.2 The CONFLUENCE Model

One of the motivations behind the proposal of a model oriented to integration of HiTLCPSs within the context of smart cities is sustainability. As evidenced in Nunes et al. [2015] and Fernandes et al. [2020], HiTLCPSs aim to generate a positive influence on individuals. However, most of these systems operate in isolation in a particular ambience and are limited to the data generated within that particular environment. While each of these systems could individually contribute to sustainability in a smart city context, interoperability between them would allow for a substantial contribution at the city level with the improvement of current services and even the deployment of new ones.

The purpose of the model is to be implemented in the context of smart city sustainability, which involves meeting current needs while ensuring the ability of future generations to meet their own needs. Sustainability encompasses three pillars: environmental, social, and economic, which are interconnected and interdependent [Purvis et al., 2019]. Figure 4.1 illustrates this connection.

Environmental sustainability focuses on preserving natural spaces and ecosystems. In the context of smart cities, there is an emphasis on utilizing green spaces and developing technologies that minimize pollution and manage resources effectively. This includes recycling, promoting green spaces, and encouraging sustainable transportation options like bicycles [Almalki et al., 2021].

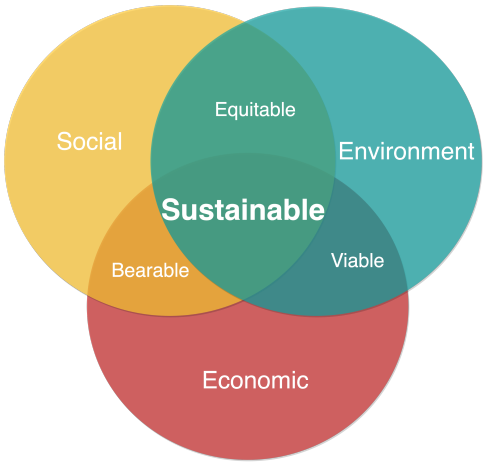


Figure 4.1: The three pillars of sustainability. Adapted from [Purvis et al., 2019].

Social sustainability places the community as a central actor in the model. It aims to involve citizens actively in technology and reduce the costs of specific technologies while promoting human participation. The model seeks to create a sense of ownership and responsibility toward sustainable practices by engaging the community [Ramírez-Moreno et al., 2021; Almalki et al., 2021]. From an economic perspective, the model aims to establish a reliable and secure framework that allows third-party organizations to support and sponsor the implementation of this technology in cities. The goal is to create a sustainable incentive structure that encourages the integral contribution of the community through green activities while ensuring economic viability.

In this sense, our proposed model - named CONFLUENCE, seeks to provide a solution for the integration of various HiTLCPSs used in a smart city, so that they can eventually interoperable, considering proactive data protection by citizens as a fundamental pillar of its design. The architecture of this model is composed of a set of entities, components, and interactions, as illustrated in Figure 4.2. The following subsections will provide a detailed description of each part of the model.

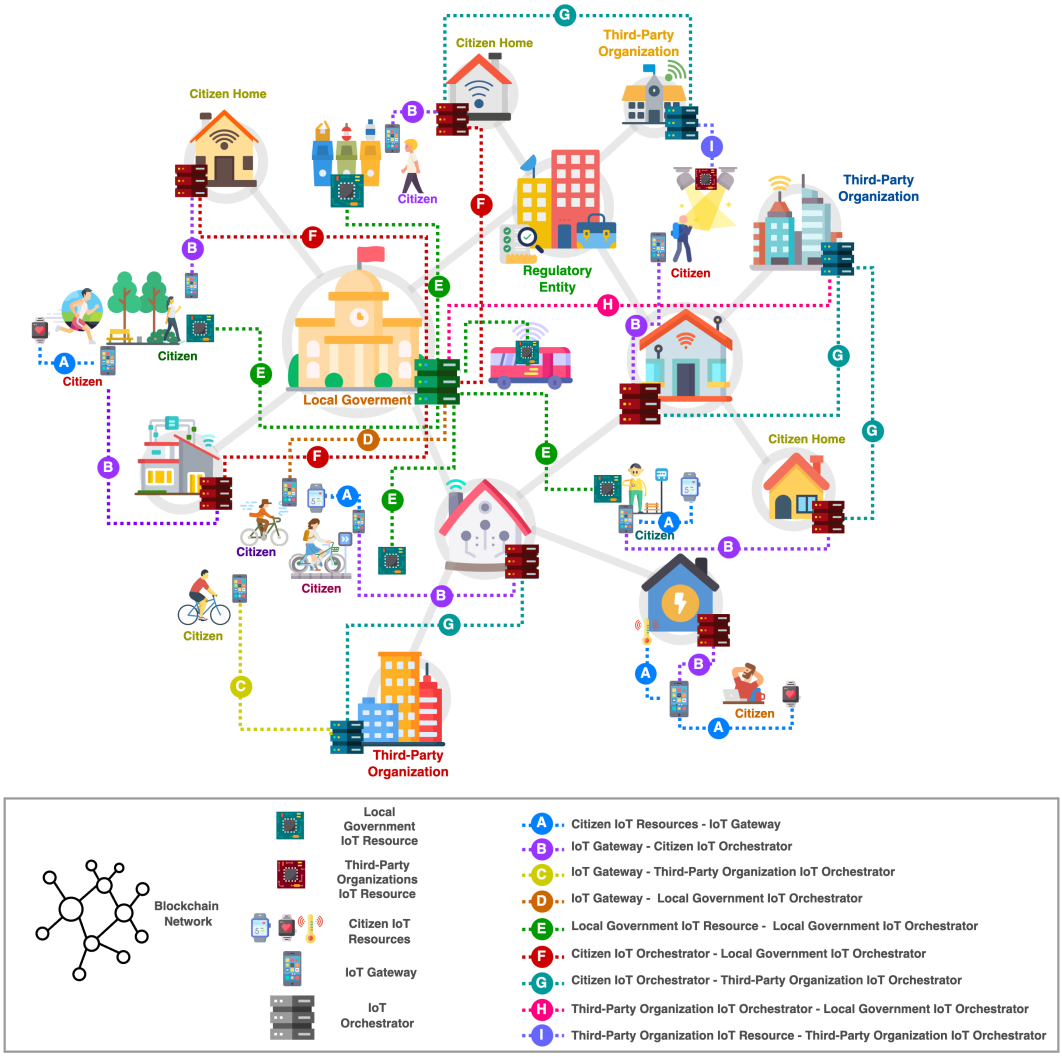


Figure 4.2: The CONFLUENCE model: entities, components and interactions.

4.2.1 Entities

4.2.1.1 Citizen

This entity is the first stakeholders within a smart city, and its participation is active, both in the interaction with services provided by HiTLCPS and in the management of its data coming from its IoT resources. This entity is typically assigned the role of DO ; however, there may also be times when its role is that of a DR .

4.2.1.2 Local Government

It is the second stakeholder in a smart city. Its functions include intermediation between entities and first-level regulation of services proposed by third-party organizations. To this end, the design, execution, and development of public policies and infrastructure to support IoT services are necessary. This entity fulfills the mixed role of the DO and DR because it can manage the data of its IoT resources distributed in the city, as well as offer services that depend on citizens' data.

4.2.1.3 Third-Party Organizations

These group stakeholders form the third entity in the model. Their role is to implement HiTLCPSs in the city and collaborate with the local government to promote sustainability. Similar to local governments, this entity implements technological infrastructure to deliver services. However, the deployment of IoT resources is limited to their environment. In this model, the main role assigned to this entity is that of a DR ; nonetheless, it may eventually also act as a DO.

4.2.2 Components

4.2.2.1 IoT Resources

These are the physical or virtual elements that generate IoT data. This model defines two types of resources: public and private. On the one hand, public IoT resources are managed by the local government and distributed across the city. Some of these resources comprise small systems meant for citizen interaction. On the other hand, the second category comprise the private IoT resources managed by citizens or organizations. Citizens' resources can accompany them during their daily routine (e.g., sensors in their wearables or personal devices) or remain within a personal context (e.g., sensors inside a smart home). In the case of organizations, resources are distributed only within their environments (e.g., devices or sensors installed in an academic institution).

4.2.2.2 IoT Gateway

This component allows citizens to register and manage their IoT resources and it also structures and funnels all the data produced by them. As an exclusive element of this entity, it has interfaces designed to support the interactions between the user and its technological infrastructure, without neglecting aspects related to the protection of their data.

4.2.2.3 IoT Orchestrator

This is a common element across all entities and allows interaction between them. Depending on the entity, the component has its own features and functions. For instance, in the case of third-party organizations and local governments, this

component enables the registration of IoT resources, a function performed by the IoT Gateway on the citizen's side. However, a common feature among all entity orchestrators in the CONFLUENCE model is that they act as nodes in the BN.

4.2.2.4 Blockchain Network

It is a network formed by a set of peers or nodes to maintain and synchronize a shared registry of digital transactions without the need for a central authority or intermediary. The nodes of this blockchain execute a set of pieces of code known as smart contracts, where rules and business logic are defined.

4.2.3 Interactions

CONFLUENCE is a model that involves multiple M2M interactions among its various components, as illustrated in Figure 4.2. The first set of interactions pertains to IoT resources, where data generated by these elements are funneled to their corresponding IoT Gateway (Interaction A). Notably, the IoT Gateway also allows citizens to register and manage their IoT resources in addition to its data collection function. By contrast, local governments and third-party organizations receive data from their respective IoT resources through their interactions with the IoT orchestrator (Interactions E and I, respectively).

The second set of interactions involves the IoT Gateway, with the most common being between it and its citizen orchestrator (Interaction B). In this case, the collected resource data are sorted, stored, and made available for sharing, based on user preferences. Citizens can choose which resources can be directly shared, select those that require consent-based data sharing, or keep apart those that are not for public access. The citizen orchestrator is designed as part of a household's technological infrastructure and should support multiple users (e.g., members of a family). A less common, but possible, scenario involve an IoT Gateway linking directly to the local government or third-party organization orchestrator (Interactions C and D). This interaction may take place, for instance, in a participatory sensing task as part of a subscribed service in which data from some personal IoT resource are yielded by the citizen. Such interactions are voluntary and can only occur if the citizen allows it, because by default, the IoT Gateway will always seek to link to its corresponding orchestrator.

The last batch of interactions (F, G, and H) involves IoT orchestrators. Interactions F and G occur between the citizen's orchestrator and others during enrollment in a service, accessing open data provided by other entities, or during data-sharing processes. Local government and organization orchestrators (Interaction H) may interact during the service registration processes or data sharing between the two entities. It is essential to note that entities can only share data from their IoT resources and not data obtained from another entity, unless there is prior consent or agreement to support such an action. To keep a track of all interactions involving data sharing or related processes, they are recorded in the blockchain to ease auditing by the RE and provide transparency

to the rest of the entities.

4.2.4 Privacy preserving data sharing

For the data-sharing process, the model components consider the characteristics defined by PACHA, the privacy-preserving framework addressed in section 3.2.1. This theoretical approach proposes a complete privacy-preserving data-sharing architecture between DOs and DRs, and defines two main elements: the privacy orchestrator and the privacy interagent. Both elements are based on modular architecture, as shown in Figure 3.2, and each module fulfills a specific function.

The original idea for the PPO was to act as an intermediary that would provide infrastructure to DRs to host and expose their services. This component offers a controlled alternative for accessing the DO collected data based on a consent process to the rest of the DRs that are not assigned the role of service providers. Nonetheless, in our model, the characteristics of the PPO were inherited by IoT Orchestrators from the stakeholders.

The PPI component allows DO to interact with the PPO via its IoT resource management and privacy preference modules. It also allows access to services from specific DRs. In our model, these capabilities are also part of the IoT Gateway.

Lastly, but certainly not least, our new proposal involves storing interactions generated within consent management processes, data sharing processes, and interactions between citizens and various IoT resources in a decentralized registry. This provides more transparency and makes it easier to audit and ensure compliance.

4.2.5 Re-Encryption Scheme

This proposed model primarily focuses on data generated by devices closely associated with citizens, as they constitute the majority within a city. Previous research indicates that from this data, various sensitive aspects of the user can be inferred [Kröger, 2019; Kröger et al., 2019]. Therefore, it becomes imperative to implement privacy-preserving measures. One effective approach is to ensure the confidentiality of information during a consented data-sharing process. By doing so, the data can be securely shared and processed exclusively by authorized entities or entity.

Within this model, the components and interactions are described in such a way that IoT gateways serve as conduits for the data generated by citizens' IoT resources, primarily directing it toward their IoT orchestrators (interaction B). The IoT orchestrators not only facilitate interactions among different entities but also play a pivotal role in the data-sharing process. Initially, they act as custodians of this information, owing to their storage capacity. Moreover, they serve as the primary contact point for other entities seeking access to the data generated by citizens' resources (interactions F and G).

While a citizen IoT orchestrator is designed to operate within a familiar environment, it remains crucial to establish robust security measures. Hence, it is deemed essential to encrypt all the information collected by this component right from its source, ensuring that only authorized entities can decrypt the data during the sharing process. To fulfill this objective, our model considers a state-of-the-art encryption scheme called Conditional Proxy Re-Encryption (CPRE) [Weng et al., 2009], which represents an enhanced version of the traditional proxy re-encryption scheme implemented in the model proposed in Chapter 3. Specifically, this new proposal adopts the CPRE scheme presented in Lin et al. [2022] known as Blockchain-based Condition Invisible Proxy Re-encryption (BCIPRE).

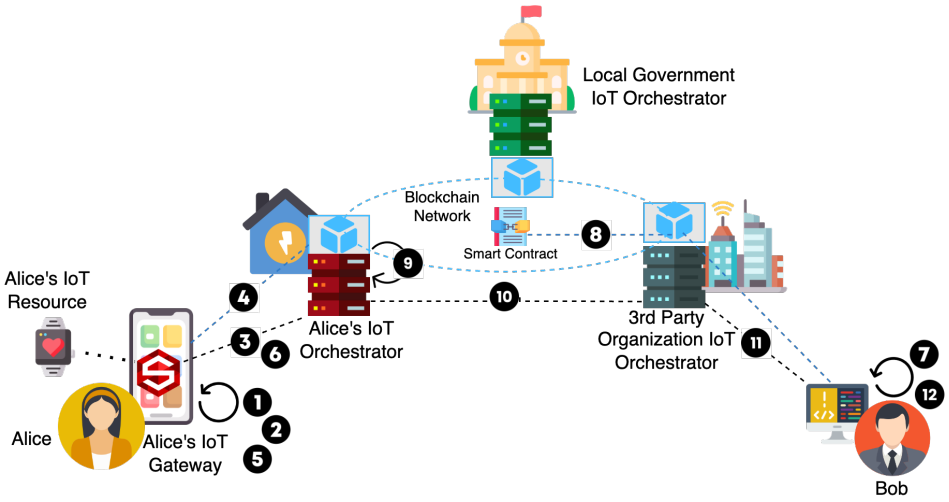


Figure 4.3: The Blockchain-based Condition Invisible Proxy Re-encryption scheme adapted to the CONFLUENCE model for a secure data sharing event between Alice (a citizen) and Bob (a member of a third-party organization)

In the example depicted in Figure 4.3, we have Alice on the left side with her IoT Gateway, responsible for collecting and organizing data from her IoT resources. This IoT Gateway is associated with Alice's corresponding IoT orchestrator, enabling various functionalities, including granting consent to members of other entities who seek access to her data. On the right side, we have Bob, who has obtained prior authorization through the consent process, as described in section 3.2.4, to access specific data from Alice's IoT resource.

The process starts with the generation of the cryptographic material (private keys and public keys) from the different entities that make up the model. In this case, Alice (Sk_A and Pk_A) and Bob (Sk_B and Pk_B).

This generation also includes global security parameters (derived from a security parameter k), as well as the sharing of the public keys.

After the collection and organization of IoT resource data over a defined time period, the IoT Gateway proceeds with the extraction of a keyword (w) from each set of data (Step 1). Using Pk_A the IoT Gateway encrypts the data (m)

Table 4.1: Additional Notation

Notation	Type	Description
e	Global security parameter	Bilinear map $e : G \times G \rightarrow G_T$
q		Prime number
G, G_T		Groups of order q
f, h		Random generators $f, h \in G$
H_1		Hash function $H_1 : \{0,1\}^* \rightarrow G$
H_2		Hash function $H_2 : \{0,1\}^* \rightarrow Z_q^*$
id_α	Global identity	id_α : identity of user α
$a_\alpha, b_\alpha, t, s, r$	Group elements	$a_\alpha, b_\alpha, t, s, r \in Z_q^*$
S_{k_α}	Private Key	Private key of user α $S_{k_\alpha} = \left(S_{k_{\alpha_1}}, S_{k_{\alpha_2}}\right)$ $S_{k_{\alpha_1}} = a_\alpha, S_{k_{\alpha_2}} = b_\alpha$
P_{k_α}	Public Key	Public key of user α $P_{k_\alpha} = \left(P_{k_{\alpha_1}}, P_{k_{\alpha_2}}\right)$ $P_{k_{\alpha_1}} = f^{a_\alpha}, P_{k_{\alpha_2}} = h^{b_\alpha}$
$Rk^w_{\alpha\rightarrow\beta}$	Re-encyption Key	Re-encryption key generated by user α to user β $Rk^w_{\alpha\rightarrow\beta} = (R_{k_1}, R_{k_2}, R_{k_3})$

(Step 2), resulting in the generation of a ciphertext (CT) and the corresponding keyword index (I_w).

$$CT = (C_1, C_2, C_3, C_4, C_5) \tag{4.1}$$

$$I_w = (C_1, C_4) \tag{4.2}$$

Each of the components of the CT and the I_w is calculated as follow:

$$C_1 = Pk^r_{A_2} \tag{4.3}$$

$$C_2 = f^{\frac{s}{r}} \tag{4.4}$$

$$C_3 = Pk^s_{A_1} \times f^{-s \times H_2(id_A)} \tag{4.5}$$

$$C_4 = e\left(h, H_1\left(w\right)\right)^r \tag{4.6}$$

$$C_5 = m \times e\left(h, f\right)^{-s} \tag{4.7}$$

Afterwards, the CT is transmitted to the IoT orchestrator for secure storage (Step 3). Simultaneously, the associated I_w is preserved within the BN ledger

(Step 4).

Following this, the IoT gateway proceeds to generate the re-encryption key ($Rk^{w}_{A\to B}$) associated with the CT. This is achieved by using Alice's private key, part of Bob's public key, and w (Step 5), as follows:

$$Rk_1 = Pk_{B_2}^{\frac{1}{Sk_{A_1}-H_2(id_A))}} \tag{4.8}$$

$$Rk_2 = H_1(w)^{\frac{1}{Sk_{A_2}}} \tag{4.9}$$

$$Rk_3 = e(H_1(w), h)^{\frac{1}{Sk_{A_1}-H_2(id_A))}} \tag{4.10}$$

Once $Rk^{w}_{A\to B}$ is generated, it is sent to the IoT Orchestrator (Step 6).

On the side of the third-party organization, Bob generates a trapdoor T_w by employing part of his private key in combination with the w (Step 7).

$$T_w = H_1(w)^{\frac{1}{Sk_{B_2}}} \tag{4.11}$$

This trapdoor is then evaluated by a smart contract within the blockchain network (Step 8). If $e(T_w, C_1) = C_4$ is met, then the corresponding I_w is sent to Alice's IoT Orchestrator. This index enables the IoT Orchestrator to retrieve the encrypted data for re-encryption using $Rk^{w}_{A\to B}$. As this key incorporates the w, the IoT Orchestrator is restricted to re-encrypting only the data that includes the keyword, thereby ensuring effective control over the data (Step 9). The resulting re-encrypted ciphertext $CT_B = (C_1', C_2', C_3', C_4', C_5')$ can be obtained through the following process:

$$C_1' = Rk_1^t \tag{4.12}$$

$$C_2' = C_3^{\frac{1}{t}} \tag{4.13}$$

$$C_3' = C_3 \tag{4.14}$$

$$C_4' = Rk_3^t \tag{4.15}$$

$$C_5' = C_5 \tag{4.16}$$

Ultimately, the re-encrypted text CT_B is transmitted to the IoT Orchestrator of the organization (Step 10), and subsequently relayed to Bob (Step 11). Bob can successfully decrypt the data m (Step 12) using his private key. The decryption process involves the following steps:

$$m = C_5' \times e(C_1', C_2')^{\frac{1}{Sk_{B_2}}} \tag{4.17}$$

As previously mentioned, this model incorporates the BCIPRE encryption scheme introduced in Lin et al. [2022]. The authors of this scheme provide a comprehensive description of the solution and conduct a formal security analysis, demonstrating its adherence to essential security properties namely collusion resistance and non-transferability.

4.2.6 Incentives Mechanism

One of the main challenges of HiTLCPSs is user involvement. Occasionally, the lack of participation is mainly due to the absence of personal data protection mechanisms, the development of artifacts without considering human-computer interaction approaches, and the scarcity of incentives. When these systems are intended to operate in isolation or interoperate in a smart-city context, it is imperative to massively increase their use. And thus these challenges must be addressed.

The first two challenges have been considered both in the proposal of the model and at the time of the implementation of the IoT gateway, the latter being the main component of interaction with citizens. For the third challenge, we propose an improvement to the incentive mechanism presented in our case-study [Sanchez et al., 2022].

In that proposal, citizens can benefit from exclusive services and discounts in retail stores by interacting with IoT resources, including a mobile application managed by the local government. This central entity assigns a point to a citizen each time he or she interacts or participate in a defined activity. The greater the participation, the more points citizens can earn. At the end of each month, citizens with the highest scores can trade their points. For the redemption process the citizens generates a QR codes to preserve their identity. However, those codes must be validated by the local government before accessing benefits.

In this new proposal, we introduce a mechanism that improves and makes the allocation of points transparent and eliminates the need for the citizen to use and validate against the local government (or any incentive provider) a code generated prior to obtaining the benefit. Owing to the use of a smart contract, every time a citizen interacts with an IoT resource within the context of a defined activity, the smart contract is invoked by the node in charge of managing the resource and the interaction is recorded as a transaction within the ledger. The blockchain will keep track of the amount points its citizens have earned in the

different activities, as well as the incentives that must be registered by the sponsoring entities. This mechanism is not limited to incentives derived from interaction with local government IoT resources, as it can be implemented and work together with incentives proposed by third-party organizations. Even in the case of joint activities between different entities, it is possible to keep track of the points earned by citizens in such activities regardless of the rest of the points. For the redemption process, the smart contract periodically verifies the status of each participant and grants benefits to the top-ranked ones without requiring a face-to-face verification process.

4.3 Summary

In this chapter, we have presented a model named CONFLUENCE that incorporates contemporary technologies like Blockchain and LoRa to integrate privacy preserving citizen-centric solutions, fostering the vision of SSC. This model is the result of integrating HiTLCPSs that implement the first privacy-preserving approach proposed in our third chapter. This integration model seeks to engage the community through green activities and incentivize sustainability at an economic level. By promoting citizen engagement, utilizing green technologies, and fostering economic support, the model aims to drive sustainable development in smart cities. Hence, in technical and general terms, the entities in the model refer to a city's stakeholders, while the components represent the technological elements with predefined functions in which the stakeholders engage. The model establishes and defines multiple interactions that can take place among these components. Additionally, CONFLUENCE introduces a mechanism for incentives to encourage citizen participation and interaction with these systems. The next chapter will provide further details regarding the implementations of the components from this model and the one presented in Chapter 3.

Publications based on this chapter's work

- Rivadeneira, J. E., Sánchez, O. T., Dias, M., Rodrigues, A., Boavida, F., and Silva, J. S. (2023d). Confluence: An integration model for human-in-the-loop iot privacy-preserving solutions towards sustainability in a smart city. *Submitted to IEEE Internet of Things Journal* **(Q1)**;

Chapter 5

Case Studies and Engineering of the Testbed

Contents

The development and widespread deployment of IoT systems that handle personal information are an inevitable trend as our society embraces higher levels of information-based systems. In this chapter, we delve into our two case studies that exemplify the implementation of the HiTLCPS concept. Each of these case studies revolves around the deployment of distinct platforms, each tailored to address different objectives in specific contexts. Subsequently, we introduce SPACES, an implementation solution that aims to integrate the services offered by the aforementioned case study platforms. However, this time, considering the privacy-preserving features of the model proposed in Chapter 3. Furthermore, this implementation will serve as a Proof-of-Concept (PoC) artifact for our integration model - CONFLUENCE - introduced in Chapter 4. This chapter provides technical details regarding the development of these components and the underlying technology used to implement this new testbed.

5.1 Group Case Studies

5.1.1 ISABELA

The IoT Student Advisor and BEst Lifestyle Analyzer (ISABELA) is our first case study designed for an educational domain. Its aim is performing a continuous students' lifestyles monitoring to infer their academic progress and try to assist them in their daily routine to enhance their academic performance, prevent failing grades, and decrease school dropout rates. From a technical perspective, this case study comprises a platform that implements the HiTLCPS concept [Fernandes et al., 2020], and its architecture is depicted in Figure 5.1. ISABELA has already been used in some field trials in different venues, both in Portugal and Ecuador with more that 40 participants per trial [Fernandes et al., 2019, 2020]. It is worth noting that the primary obstacle to widespread participation, as highlighted by the students, is the assurance of their privacy.

ISABELA's platform comprises services and operates using smartphones running a mobile app, wearable devices and IoT Boxes (hardware components that integrate environmental sensors) to gather data. These data, mainly originated from physical sensors, electronic-based sensors, and OSN [Armando et al., 2018] is then processed by a core infrastructure to figure out students' emotions, intents, and actions. This modular infrastructure is an arrange of elements based on FIWARE Generic Enablers (GEs).

5.1.1.1 FIWARE

FIWARE is an open ecosystem for experimentation that has emerged in response to the dynamic landscape of the information technology market [Sinche et al., 2020a], simplifying:

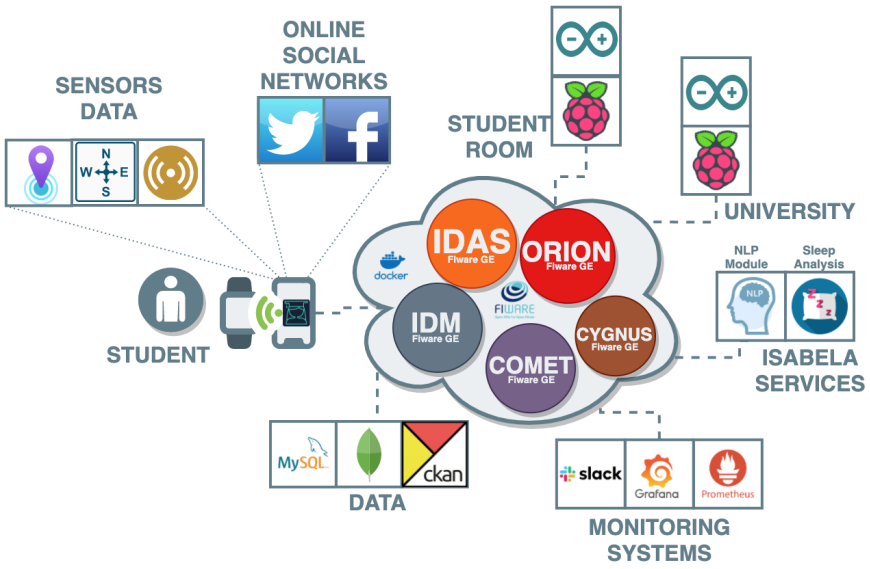


Figure 5.1: ISABELA's platform architecture. Adapted from Fernandes et al. [2019]

- The development of applications in the Internet of the future.
- The hosting capacities and access "as a service" to the functions that facilitate the connection with the IoT.
- The management and knowledge processing (context information) and the analysis of large-scale multimedia content in real time.
- The incorporation of advanced functions in user interfaces, among others.

FIWARE, from a streamline perspective, presents an interconnected node infrastructure formed by Backbone, Network, Computing, Storage and Scalability Power. This middleware offers an open and standardized platform and a set of GEs.

The GEs are generic, adaptable and reusable software components used as building blocks to rapidly develop specific applications and services based on the Internet of Future. These components are available in the GEs catalog of FIWARE[1].

Features of these GEs include Public Specifications available through the API and some of them are open source. Any implementation of a GE is formed by a set of components that supports specific group of functions and APIs based on the open specifications. Research centers, public and private institutions are behind the development of GEs.

GEs are classified into seven technical chapters:

- Data/Context Management
- IoT Services Enablement

[1]https://www.fiware.org/catalogue/

- Advanced Web-based user interface
- Security
- Architecture of Applications/Services Ecosystem and Delivery Framework
- Interface to Networks and Devices
- Cloud Hosting

As depicted in Figure 5.1, the ISABELA's plaform leverages IDAS, IDM, COMET, CYGNUS and ORION, from the pool of available FIWARE GE. An in-detail description of the design, development, deployment, and assessment of this HiTLCPS can be found in Fernandes et al. [2020], while a complete analysis of student academic performance based on ISABELA is described in Sinche et al. [2020a].

5.1.2 Green Bear

Green Bear, also known as 'Urso Verde' in Portuguese, is our second case study aiming to improve the city's sustainability, the lifestyle of its citizens, and the dynamics of the city. Green Bear extends the idea behind ISABELA into a smart city system context as it not only collects information of citizens extracted from their mobile phones but also enhances the experience with data obtained through the interaction of users with various IoT devices [Sanchez et al., 2022].

As our previous case study, Green Bear provides a HiTLCPS, but in this time the system comprises a mobile application interacting with LoRaWAN nodes strategically located in the city, which collect data on the users' activity. This solution includes LoRaWAN nodes using a public The Things Network (TTN) gateway, a TTN application to integrate external services, a FIWARE based back-end, a dashboard for system management, and a mobile application that integrates humans in the system. Figure 5.2 shows the overall architecture of the Green Bear solution.

In both case studies, the smartphone plays a key role, not only as a data source but as a way that the systems interact with their users. Each system offers its own application, which include a chatbot that provides recommendations on sleep hours and physical activity, depending on the user's performed activities. Notifications help participants to become more involved in the system. Additionally, the chatbot allows the system to ask questions and set mobile parameters, assisting the user in configuring the system. The overall objectives of the mechanisms implemented in the Green Bear application are to foster the citizens' interaction with city spaces, e.g., green spaces, outdoor activities, recycling dynamics, and also to incentivize the users' physical activity, sleep time, and quality of life. The latter being common in the case of ISABELA's mobile application.

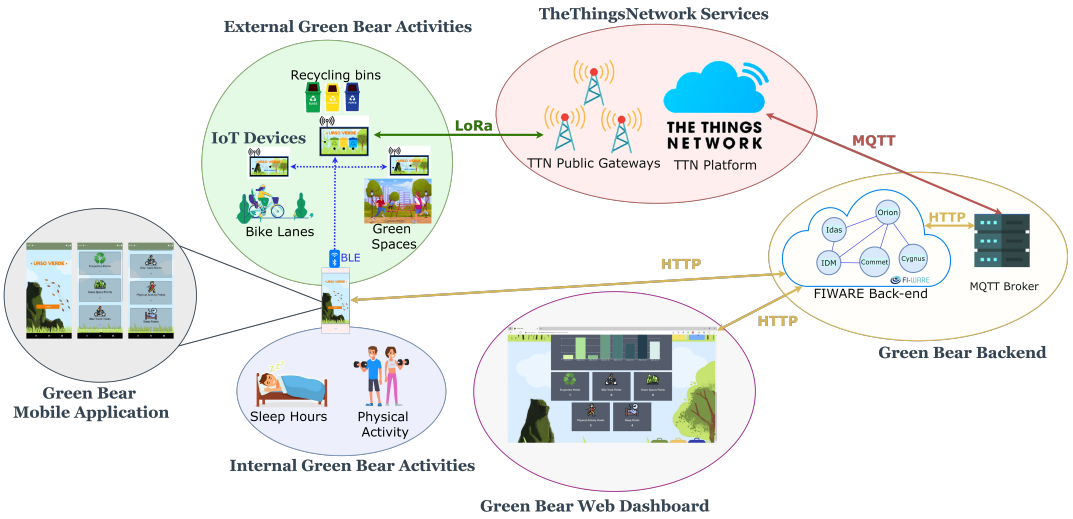


Figure 5.2: Green Bear's platform architecture. Adapted from Sanchez et al. [2022].

5.2 SPACES Platform

A common aspect of ISABELA and Green Bear platforms is the lack of user-centric data protection mechanisms. Both systems do not offer its users a way to control the data flows that are being collected and sent for inference processes. Although certain privacy aspects, such as data anonymization and the use of pseudo-identifiers, have been considered in the design of both systems, the absence of a model that empowers the end user and allows respecting the right to privacy is one of the main milestones to be met in both case studies.

In this sense, and taking into account the common points of both HiTLCPS, for the assessment of our proposed models introduced in the previous chapters, it has been decided to develop a new unified platform – named SPACES – aligned with our privacy-preserving model components (based on the PACHA framework) and with the aim of integrating various services derived from the HiTLCPS previously developed.

As in ISABELA and Green Bear, this new platform leverages users' smartphones, IoT Boxes, and other hardware elements to represent the components of our proposed models. In this section, we present the implementations descriptions of these components, including details of the underlying technology that allowed the implementation of these components.

5.2.1 IoT Broker, IoT Orchestrator and IoT Gateway

Both, the IoT Broker (first model) and the IoT Orchestrator (second model) implement the modules proposed by the PPO. However, in the case of the IoT Orchestrator, depending on the entity, the number of modules varies, but in general, all orchestrators implement the Data Acquisition Module (DAM), the Consent Manager (CM), a Privacy Enforcement Bridge (PEB), a Data Requests

and Subscription Module (DRSM), and the Data Dispatcher Module (DDM). In the case of the local government and the third-party organizations, their orchestrators implement the IoT Service Providers Repository (ISPR), the IoT Services Diffusion (ISD) module and an extra module for IoT Resource Management module.

To implement these modules and their functions, services were developed using JavaScript through NodeJS, while certain modules were enhanced with the existing features offered by the FIWARE GEs.

In our implementation the identity management feature of the ISPR is carried out by Keyrock-GE. A core part of DDM and the DRSM is the Orion Context Broker-GE, while for data acquisition from IoT gateways, DAM relies on IDAS-GE. Apart from GE, some third-party solutions were integrated within the implementation of this component. For instance, in the case of ISD, Firebase Cloud Messaging is used to ease the generation of notifications for the agents, while JSON Web Token (RFC 7519) is used for token issuing. In the case of the IoT Orchestrator from the local government the DAM implements also a Message Queuing Telemetry Transport (MQTT) client.

In addition to their own functions, each of these modules exposes a set of APIs, which provides flexibility and interoperability between the various modules.

In the case of the IoT Gateway from both models, this component implements the modules comprising the PPI plus an IoT Resource Management Module. This latter module allows the DO to pick up and control which resources are going to be part of the consent and data release process. The modules with user-interaction capabilities are implemented in a smartphone application developed in Xamarin (C#) to ensure cross-platform compatibility (Figure 5.3). In the case of the IoT Gateway from our first model, the modules that perform actions that do not depend on user interaction were developed as microservices in JavaScript, integrating existing libraries like crypto-js, bcryptjs, and recrypt-js. Also, this IoT Gateway instantiates Orion Context Broker-GE and IDAS-GE for data management functionalities, complementing the functions of the developed modules.

As in the case of the IoT Gateway, the DR system implements a lightweight version of the PPI instance. This version is comprised of a consent request module, a compact notification module, and a privacy policy and security module. In particular, the consent request module supports the DR to select simultaneously different IoT resources from the same DO or from different ones.

All these modules were written in JavaScript through NodeJS and provide a set of APIs. However, to fulfill the interactive features of the consent request and notification modules of this PPI version, it includes a front-end application developed using React (Figure 5.4).

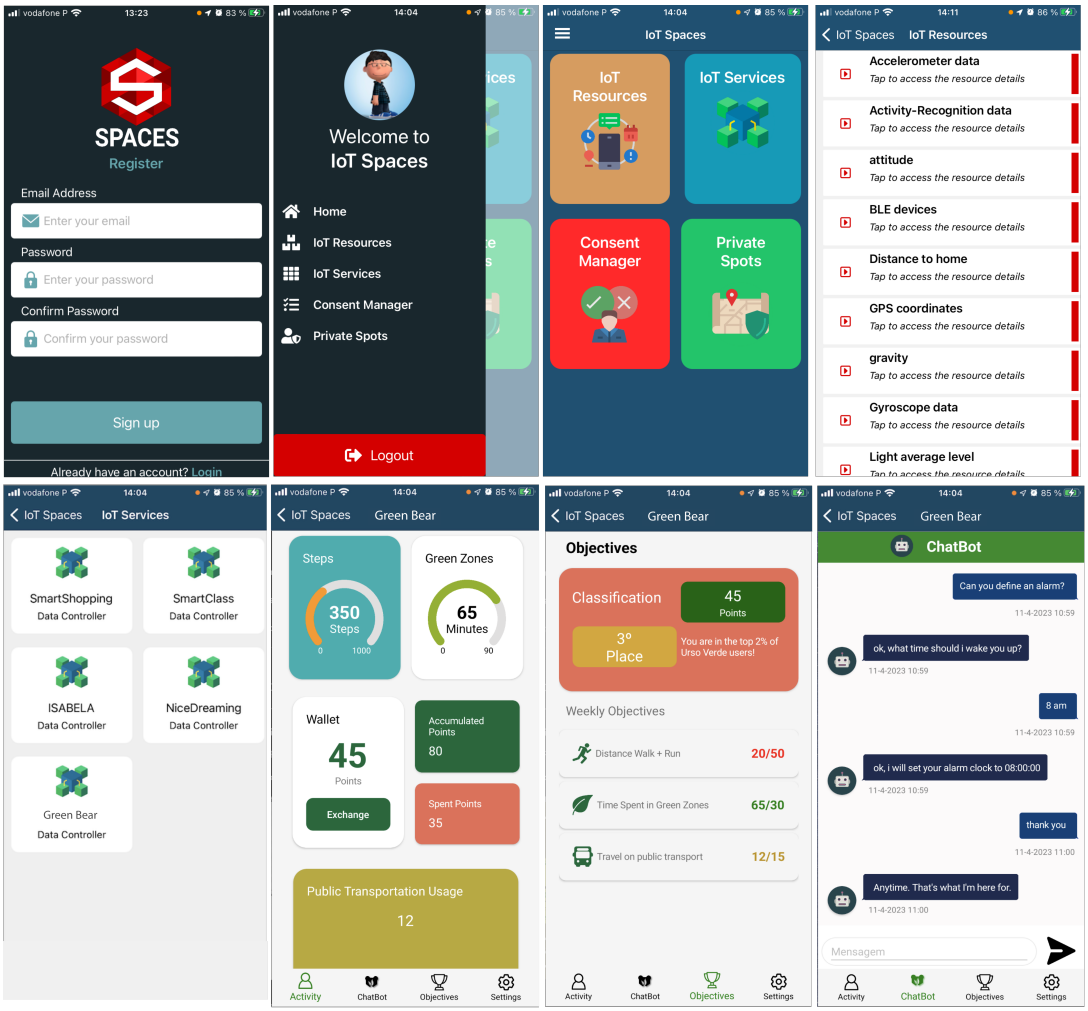


Figure 5.3: SPACES Mobile Application as part of the IoT Gateway component.

5.2.1.1 HiTL-IoT based Services

The Green Bear services are included in the pool of HiTL-IoT based services that the IoT Gateway's implementation offers and in the case of our second model, as already mentioned its aim is to promote sustainable living habits among citizens namely encouraging recycling, the use of bicycles, using public transportation, and participating in voluntary actions.

To develop this service, we identified functional requirements by considering the target audience (in our case, citizens) and the desired features. This service encompasses several features and components, such as activity tracking, objectives displaying, a chatbot, a QR code validator, and a BLE advertiser. To encourage participation, the service implements a point-based reward system called Citizen Points based on our proposed incentive mechanism.

For implementing this service, we have followed an agile methodology, particularly the principle of "working software over comprehensive documentation" [Wagenaar et al., 2018] and the practice of "code reuse" [Frakes and Kang, 2005], this involved employing a code reuse approach, which entails adapting previous

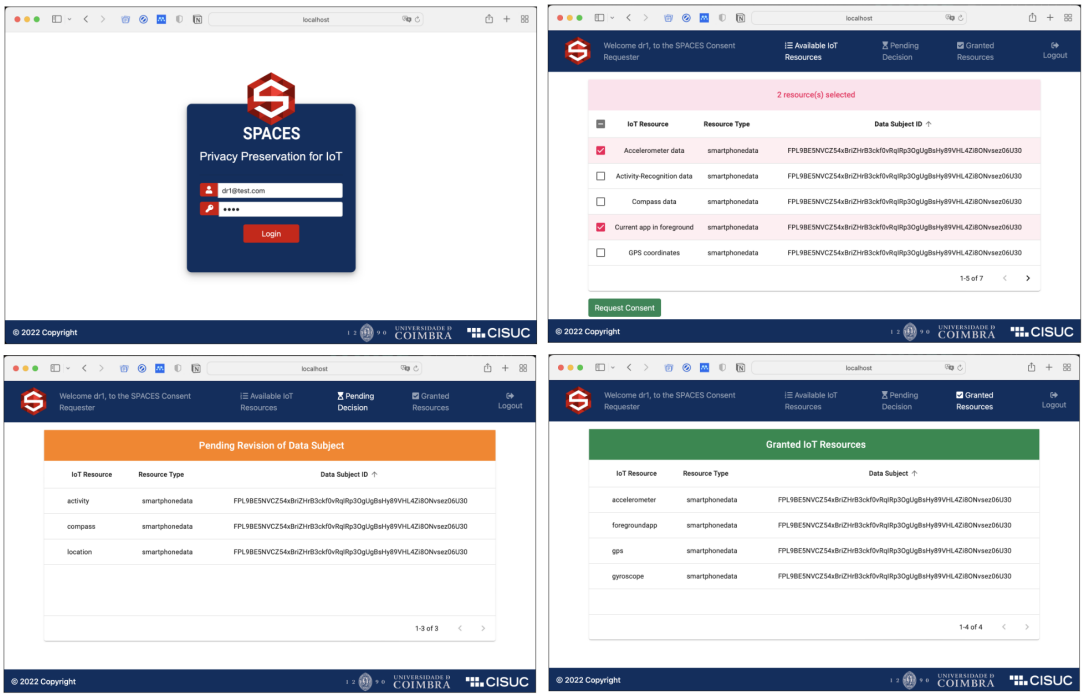


Figure 5.4: SPACES front-end application developed in React for DR consent requesting.

code to enhance the efficiency and efficacy of the development process.

One of the services' capabilities is to communicate with public IoT resources through a BLE advertiser to validate user actions. For instance, when a citizen performs a recycling task and interacts with a public IoT resource (e.g., pressing a button), this resource is capable of fetching the advertised user pseudo ID from the IoT Gateway to validate the interaction. Later, the collected data are sent to the IoT orchestrator for the Citizen Point assignment.

However, there is another validation method supported by this service. Through the QR validator, the actions of the citizens can be verified instead of interacting directly with the hardware of IoT resources. For example, after completing a task, the IoT resource can generate a QR code, and a citizen leveraging this smartphone camera can read the QR code to validate the action.

To provide the citizens with a friendly interaction interface, this service implements three main views: Activity, Chatbot, and Objectives (Figure 5.4). The first view displays charts with user activity metrics, such as steps taken, time spent in green zones, and the number of Citizen Points (accumulated and spent).

The second view retrieves the objectives and shows the user's Citizen Points, as well as their classification. Each objective is color-coded to show the progress, with red indicating that the objective is far from completion, yellow indicating that it is almost complete, and green indicating that the objective is complete. In addition to the weekly objectives, there are monthly objectives. These tasks are typically difficult to complete and may require more effort from citizens,

such as through voluntary work. However, they offer more points and can be a great way to earn rewards through the Citizen Points system.

The Chatbot view provides users with a convenient and user-friendly way to ask questions and receive feedback regarding their activities. Using Dialogflow[2], the Chatbot can analyze citizen intents and provide accurate and relevant answers to their queries. This is achieved through machine learning algorithms that enable the Chatbot to recognize and interpret natural language inputs from users, allowing for more natural and conversational interaction. In the future, the integration of ChatGPT with Dialogflow could further enhance the user experience by allowing for more complex and engaging conversations.

HiTL-IoT services like Green Bear, play a crucial role as catalysts for human-system interaction, necessitating the design of a citizen participation platform. This platform supports sustainable initiatives, enabling individuals to provide real-time feedback on system usage and its proposed activities. Furthermore, HiTLCPS, such as the one proposed, enable interventions to promote sustainable behavior among citizens. These interventions specifically aim to encourage sustainable practices related to outdoor activities and recycling. Also, implementing and integrating the Green Bear service represents a significant milestone in developing the IoT Gateway to promote sustainable living habits. Finally, the incentive systems within the proposed framework aim to facilitate the generation of green businesses and investments by local companies, leveraging citizen points as a mechanism. By incorporating a transparent scheme, the platform minimizes investment risks for companies, thereby supporting the transition toward sustainable habits within the city. Furthermore, as observed in Xiao et al. [2022], gamification systems have effectively motivated user participation, leading to higher acceptance rates and improved performance of systems.

5.2.2 IoT Resources

In the case of our first model, the platform leverages the internal sensors of the DO handheld device as IoT Resources. However, the nature of our second model required the implementation of new resources in addition to those previously mentioned. These resources are classified into two groups. The first one presents the development of an IoT resource intended to be implemented by a local government while the second one is oriented toward an IoT resource within a third-party organization.

5.2.2.1 Local government IoT resource

As indicated in the previous chapter, public IoT resources are distributed around a city and must be ready to interact passively or actively with citizens. In addition to their functionalities, deploying these devices outside a controlled environment brings challenges, such as communications with the orchestrator and power supply.

[2]Dialogflow: https://cloud.google.com/dialogflow/docs?hl=en-en

These devices collect data and transmit it to a central system. The nodes were created using Pycom devices with a microcontroller that can be programmed using Micropython. Pycom FiPy devices provide connectivity options for LoRaWAN and BLE, enabling the development of flexible systems with diverse communication capabilities. These devices are based on ESP32 SoC and offer low power consumption, 4MB RAM, 8 MB Flash Memory, and various peripherals suitable for IoT applications. Moreover, the Pycom firmware permits developers to use several microcontroller functions such as interrupts, timers, analogue-to-digital converters, digital-to-analogue converters, and general-purpose input/output pins, among other features.

Furthermore, by placing IoT devices in strategic locations, the accuracy and reliability of environmental and activity measurements can be ensured, and citizens can be incentivized to participate in smart city initiatives. This participatory approach helps from both sustainability and community engagement perspectives. The devices use BLE to interact at close range with citizens' IoT gateways. In addition, considering our previous work [Sanchez et al., 2022], we kept the frame format within the PDU advertisements, communicating the pseudo-identifier or user pseudo ID through 2 bytes, which will be determined through the users' application. While for long-distance communication, the devices use LoRaWAN, which similarly maintains the 3-byte format, as in Sanchez et al. [2022], communicating the 2-byte pseudo-user ID plus one additional byte for device identification and functionality. Using BLE for communication can help minimize the energy consumption of IoT resources and users' mobile devices when notifying activities defined by the local government.

These public IoT nodes consist of a Pycom device, LiPo battery, developing board, LoRaWAN antennas, and control buttons to trigger node operations. Figure 5.5 provides an overview of the appearance of the LoRaWAN nodes. These devices operate in sleep mode until a user activates them by pressing a control button, which triggers an interruption and wakes them up. Once the node has awakened and the pin handler has been activated, it passes the type of activated button to a function that initializes BLE within the node that processes the user pseudo ID and saves the information to send a LoRaWAN packet with all IDs processed once a day. To keep things simple, these nodes are manually activated as a first step, though more automated approaches may be considered in the future.

The local resources devices use the public TTN, a collaborative platform that The Things Industries created for developing and deploying LoRaWAN networks, devices, solutions, and documentation. IoT devices establish LoRa communication with public gateways provided by TTN services, which are responsible for sending the collected data to the application server. This server then enables the information to be decoded and extracted using external connectors. IoT devices send LoRaWAN frames that contain identifiers and function types, and the platform structures the message for external connections. TTN also allows for the definition of payload formats in JavaScript, decodes incoming node messages, and reformats them before sending them to subscribing applications. The decoded payload is designed to establish the object format for external con-

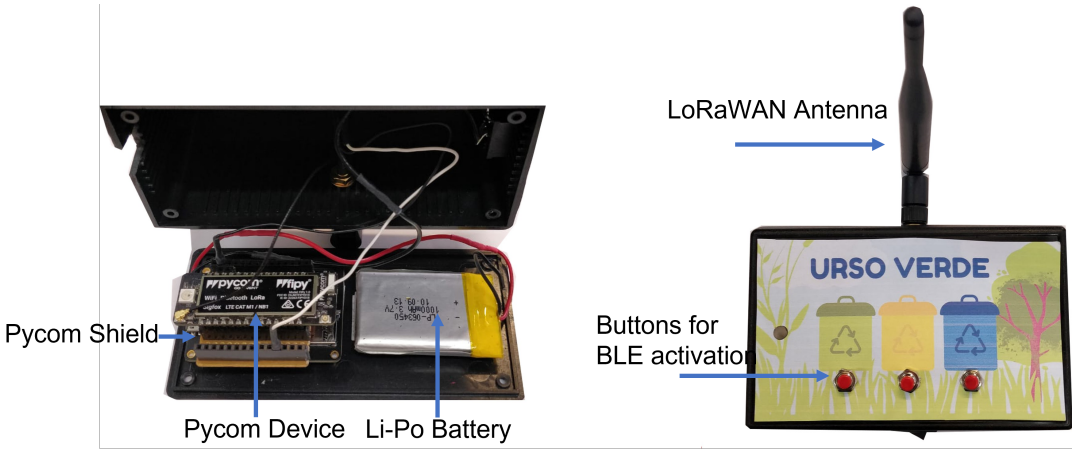


Figure 5.5: Local government IoT resource device

nections [Sanchez et al., 2022]. TTN supports MQTT connections and acts as a broker, enabling third-party applications to publish and subscribe to established topics. The subscribing upstream traffic topics include joining, data, and acknowledgement information. At the same time, TTN can push external data or commands to the nodes using the downstream topics, providing end-to-end communication between external applications and LoRaWAN nodes.

The TTN platform includes connectors that support two methods for clients: subscribing to upstream traffic and publishing downlink traffic. An MQTT broker should be considered for the local resources because it allows subscribing to the topic v3/application id@tenant id/devices/deviceid/up and extracting upcoming information provided by the devices. The prescribed information file contains all the necessary details for communication in LoRaWAN. This file includes device identifiers, application identifiers, connection identifiers, signal strength information, and decoded payload. The decoded payload is in JSON format and allows for extracting the user pseudo identifier information. This information can be used for the incentives' mechanism carry out by the local government and third-party entities.

It is worth mentioning that the design of the architecture of the components and especially of the IoT public resources was done with the active participation of the Coimbra city council. Through initiatives such as the Future City Challenge[3] in collaboration with TTN, the creation of solutions using public gateway infrastructure has been encouraged, and the chamber has allowed the installation and use of municipal spaces for the implementation of these resources. The active participation of local governments in these sustainable solutions allows these solutions to be monitored and reported for their emergence through government budgets, in addition to guaranteeing a certain commitment with public and private companies for investment in view of the viability of the systems and platforms.

[3]Future City Challenge: https://futurecity.pt/

5.2.2.2 Third-party organization IoT resource

Unlike previous IoT resources, third-party organization ones have the advantage of being deployed on their premises as part of its provided service. This is a significant advantage in terms of the connectivity and energy provision. In our case, we leverage the implementation of an IoT Box, developed for our HiTLCPS, called ISABELA [Fernandes et al., 2020].

These IoT boxes are hardware structures consisting of Arduino and Raspberry PI boards, a voltage converter, and a set of environmental sensors, including a temperature sensor (DTH11), light sensor (IM120710017), sound sensor based on an electret microphone, and LM386 amplifier (Grove M0A160719024). An Arduino board was used to process the information generated by the sensors. In the case of sound sensors, the raw information is analog, whereas in the case of light and temperature sensors, the information coming from them is digital. The Raspberry PI is used to communicate the information processed by the Arduino board via the Internet. All the data from this IoT resource is funneled by the DAM in the orchestrator through an IoT agent provided by IDAS-GE. Regarding energy supply, this IoT resource uses a voltage converter since the Raspberry Pi and Arduino operate with different voltage levels. Figure 5.6 shows the implementation of an IoT Box used to sense environmental conditions.

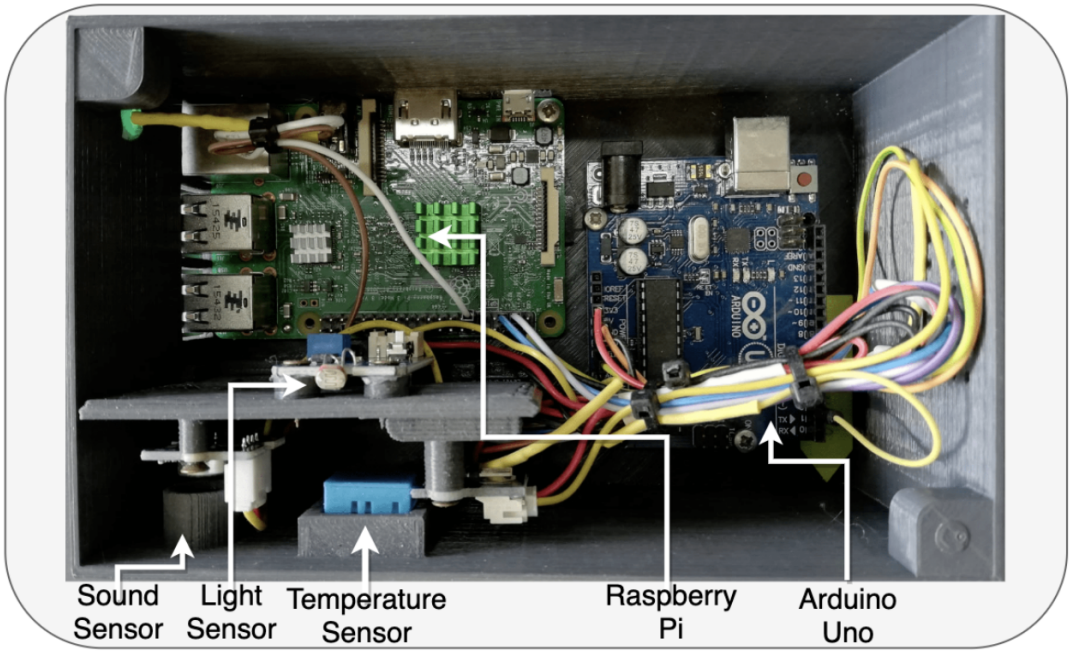


Figure 5.6: IoT Box representing a third-party organization IoT resource

5.2.3 Blockchain Networks

Both models relies on a blockchain network as one of its essential components. In fact, one type of interactions between the entities in the second model is through this component. In this sense, Hyperledger Fabric (HLF) was chosen as distributed ledger technology [Honar Pajooh et al., 2021]. HLF is a permissioned

blockchain framework supported by the Linux Foundation. This framework has been devised for the development of distributed applications with a modular architecture, allowing different networks and services to be connected in a simple and scalable fashion [Li et al., 2020]. HLF can manage large amounts of data with an outstanding performance compared to permissionless schemes. The main elements that comprise a typical HLF network are the peers, the ordering service, the channel, the chaincode and the Membership Service Provider (MSP). Table 5.1 summarizes each of these elements.

The peers and the orderers are nodes of the network with different roles but with the common goal of ensuring that the ledger is kept up to date. The main functions of the peers are threefold: keep a copy of the ledger, execute transaction proposals submitted by the client application, and validate transactions. A peer can be broadly classified as an endorser (or endorsing peer) and committer (or committing peer). The former is responsible for executing transaction proposals, while the latter saves the validated transactions into the ledger. Peers can also be categorized as Anchor peers within an organization. Anchor peers facilitate inter-organizational communication between peer nodes by utilizing the gossip protocol in HLF. Through this protocol, anchor peers locate other accessible member peers, disseminate ledger data among peers within a channel, and ensure efficient updates for newly added peers.

On the other hand, the orderers are nodes that in conjunction provide the ordering service. This service settles consensus regarding transactions order. The channel is a private communication mechanism where specific members of a network can perform transactions. Each channel deploys a ledger to record the transactions of its members. The fourth relevant element is the chaincode, directly related to the smart contract. The chaincode is a piece of software instantiated in the blockchain containing the application logic which must be invoked to generate transactions to be further recorded on the ledger. The chaincode and the peer are loosely coupled and exchange messages using Google Remote Procedure Call (gRPC). Finally, the MSP keeps the nodes' identities and issues credentials for authentication and authorization purposes [Androulaki et al., 2018]. The MSP turns verifiable identities into roles within the network and determines which Certification Authorities are approved to specify the members of a trusted domain.

In our current implementations, HLF stable version 2.2 has been selected. In the first model, the peers and the orderers are distributed across the IoT Broker, IoT Gateways, and the Data Requester Systems, while in the second model, the peers are instantiated in all the IoT Orchestrators. In the case of the ordering service, it implements RAFT, a crash fault-tolerant protocol to achieve consensus among orderers regarding the order of the transactions. All the peers form a channel, thereby they share a single ledger. The chaincode used in this prototype has been developed in JavaScript using the HLF-Software Development Kit (SDK). For this PoC, all the cryptographic material was generated a priori using the HLF cryptogen binary.

Table 5.1: Overview of key elements in a Hyperledger Fabric network

Element	**Description**
Peer	Nodes that keep a copy of the ledger, execute transaction proposals submitted by the client's application and validate transactions. Peers could be: - Endorsers: Execute transaction proposals - Committers: Record validated transactions to the ledger - Anchors: Peers on a channel that other peers can discover and communicate with.
Orderers	Nodes that provide the ordering service to settle consensus regarding the transaction order. The ordering service is implemented as a cluster of orderer nodes. HLF supports the following ordering service protocols: - Solo ordering - Kafka-based ordering - Raft-based ordering - Practical Byzantine Fault Tolerance
Channels	Private communication mechanisms that enable specific members of the network to perform transactions. Each channel deploys a ledger to record its peers' transactions.
Chaincode	A piece of software instantiated in the blockchain that contains the application logic, which must be invoked to generate transactions to be recorded on the ledger. Chaincode and peers are loosely coupled and exchange messages using gRPC.
Membership Service Provider	Responsible for keeping nodes' identities and issuing credentials for authentication and authorization purposes. It transforms verifiable identities into roles within the network and determines which Certification Authorities are approved to specify the members of a trusted domain.

5.3 Summary

On the path to validating our models, especially when following an experimental approach, the next step after their proposal is the implementation. In this chapter we began by introducing of our two HiTLCPS case studies, which has allowed us to contextualize and justify the development of our new testbed. The outcome of this implementation has enabled the transformation of our conceptual models into tangible and functional systems. The implementation process has demanded meticulous attention to detail, as each component and mechanism is carefully crafted to ensure seamless integration and adequate performance. The next chapter will provide the description of the experimental setup used, and the experiments designed to validate these models, as well as the discussion of the results obtained.

Publications based on this chapter's work

- Sanchez, O. T., Fernandes, J. M., Rodrigues, A., Silva, J. S., Boavida, F., Rivadeneira, J. E., de Lemos, A. V., and Raposo, D. (2022). Green bear - a lorawan-based human-in-the-loop case-study for sustainable cities. *Pervasive and Mobile Computing*, 87:101701 **(Q1)**;
- Rivadeneira, J. E., Jiménez, M. B., Marculescu, R., Rodrigues, A., Boavida, F., and Sá Silva, J. (2023b). A blockchain-based privacy-preserving model for consent and transparency in human-centered internet of things. In *Proceedings of the 8th ACM/IEEE Conference on Internet of Things Design and Implementation*, IoTDI '23, page 301–314, New York, NY, USA. Association for Computing Machinery;
- Rivadeneira, J. E., Sánchez, O. T., Dias, M., Rodrigues, A., Boavida, F., and Silva, J. S. (2023d). Confluence: An integration model for human-in-the-loop iot privacy-preserving solutions towards sustainability in a smart city. *Submitted to IEEE Internet of Things Journal* **(Q1)**;

Chapter 6

Assessments and Results

Contents

Once the components of our SPACES platform are implemented, which are based on the elements proposed in our previously developed models, the next step is their deployment in test environments and validation. In this regard, the first two sections of this chapter approach the evaluations from a quantitative perspective. Additionally, this chapter includes a section dedicated to a qualitative study conducted to understand the perception of trust in IoT mobile applications, a relevant aspect shared by the platforms derived from the case studies described in the previous chapter, as well as our current platform.

6.1 Privacy Preserving Model for HiTLCPS

After the SPACES platform implementation described in the previous chapter, we deployed it with the objective of assessing our proposed privacy-preserving model in a prototype setting. This section begins by describing the architecture of the testbed for this PoC. Subsequently, extensive assessment results are presented. Finally, this section identifies the differences between this proposal and existing solutions.

6.1.1 Prototype Platform Deployment - Test Environment

The test environment comprised several physical devices and virtual machines (VMs), as depicted in Figure 6.1. In this testbed, the IoT Gateways were implemented in physical machines while the IoT Broker and the DR Systems were deployed in VMs. The PPIs and the PPO of these components, along with the GE of the IoT Gateways and the IoT Broker, ran on top of Docker containers. The mobile application, with the supplementary functionalities of the IoT Gateway, was installed on two smartphones (iOS and Android devices). A fourth virtual instance represented the Regulatory Entity. All these components formed an overlay network using Docker Swarm and each one ran a HLF peer and an ordering service node. Finally, a third physical machine was used for benchmarking purposes and assessment. The technical specifications of the devices used to deploy the elements in this testbed are summarized in Table 6.1.

Table 6.1: Technical Specifications SPACES Testbed Platform Components

	IoT Gateway 1	IoT Gateway 2	SP 1	SP 2	IoT Broker	DR System 1	DR System 2	Regulatory Authority	Assessment Machine
CPU	Intel Core i3 6100 2x 3.70 GHz	Intel Core i5 3330S 4x 2.70 GHz	A10 Fusion 4x 2.34 GHz	HiSilicon Kirin 659 Cortex A53 4x 2.36 GHz	Intel Core i7 2x 3.1 GHz	Intel Core i5 10300H 4x 2.5 GHz	Intel Core i7 1165G7 2x 2.80 GHz	Intel Core i5 10300H 4x 2.5 GHz	Intel Core i7 2x 3.1 GHz
RAM	8GB	8GB	2GB	4GB	12GB	8GB	8GB	4GB	16GB

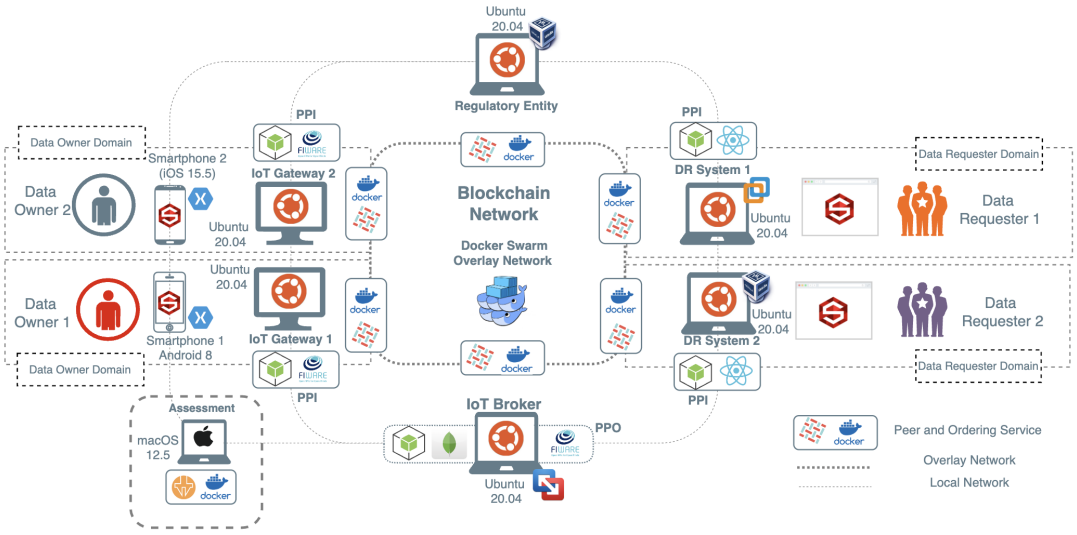


Figure 6.1: SPACES Testbed - comprising physical (including smartphones) and virtual machines to deploy the components of the model and the blockchain peers.

6.1.2 First approach assessments

The consent procedures and data sharing process from the first approach that comprise the privacy-preserving model, rely on the interaction of components with the IoT Broker and also with their peers on the blockchain network, either by reading from or writing to the ledger. Based on this premise, this assessment consists of a series of experiments to measure the response of the IoT Broker, the transaction throughput and latency of the BN and the impact of the data re-encryption process.

6.1.2.1 IoT Broker Response

Another aspect that was validated in this proposal is the response of the IoT Broker to DOs and DR requests due to the fact in a full-scale deployment, the amount of IoT Gateways and DR endpoints will always be on the rise. The IoT Broker was subjected to stress tests utilizing HTTP traffic to thoroughly evaluate its performance and scalability under demanding conditions. The stress test duration was a total of 15 minutes, consisting of nine separate intervals of varying duration and virtual user (VU). Table 6.2 describes the duration of each stage and the number of VU. We evaluated the performance under two types of HTTP requests (GET and POST). GET requests were used to retrieve data from the IoT Broker regarding the IoT services, while POST requests were used to submit the IoT data from the IoT Gateways. After the experiment, we collected performance metrics, such as response time, throughput, and error rate, to evaluate the IoT Broker performance under different load levels.

Figures 6.2 and 6.3 represent the throughput of the IoT Broker under increasing levels of load, measured in VUs, over a period of time. The Y-axis on the left shows the throughput in operations per second (ops/s), while the Y-axis on the

Table 6.2: Stress Test stages

Stage	Number of Virtual Users VU	Duration (sec)
1	Increases from 0 to 500	60
2	Remains at 500	120
3	Increases from 500-1000	60
4	Remains at 1000	120
5	Increases from 1000-1500	60
6	Remains at 1500	120
7	Increases from 1500-2000	60
8	Remains at 2000	120
9	Decreases from 2000-0	240

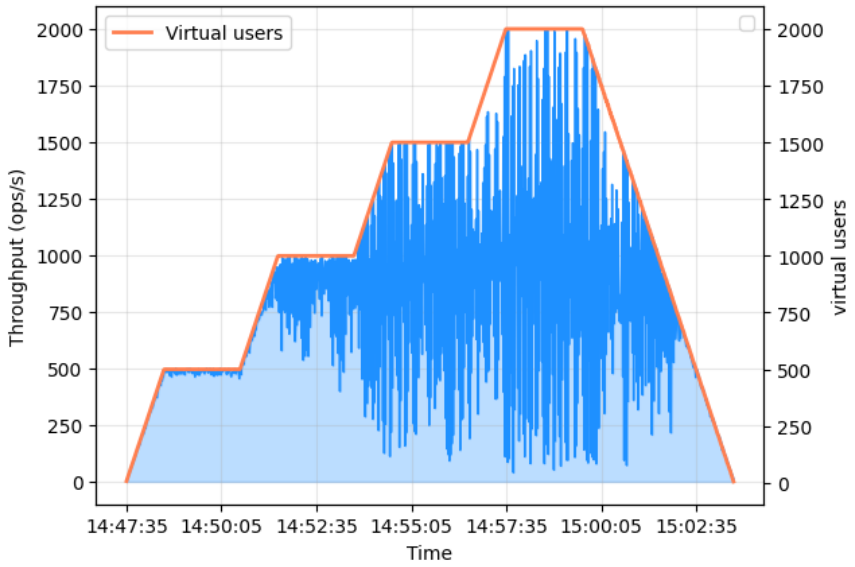


Figure 6.2: IoT Broker Throughput (POST Requests)

right shows the number of VUs. The X-axis represents the time intervals. For both types of requests, these figures show that as the number of VUs increases, the server's throughput initially rises linearly, indicating that the IoT Broker can handle the increased load efficiently. The request rate used in the experiments was 1 request per VU per second. In the case of the POST requests (Figure 6.2) after the 750 VUs, the throughput fluctuates severely compared to the GET requests (Figure 6.3), where the throughput begins to plateau with more controlled fluctuations.

Based on the same load-increasing scenario, Figures 6.4 and 6.5 show the response time and error rate of the IoT Broker, where the y-axis on the left represents the response time in milliseconds, and the y-axis on the right represents the number of error requests. It can be observed that for 750 VUs, the response time for types of requests was low and remained constant throughout the test duration. This suggests that the IoT Broker can effectively and efficiently handle a moderate number of user requests. However, as the number of VUs increases,

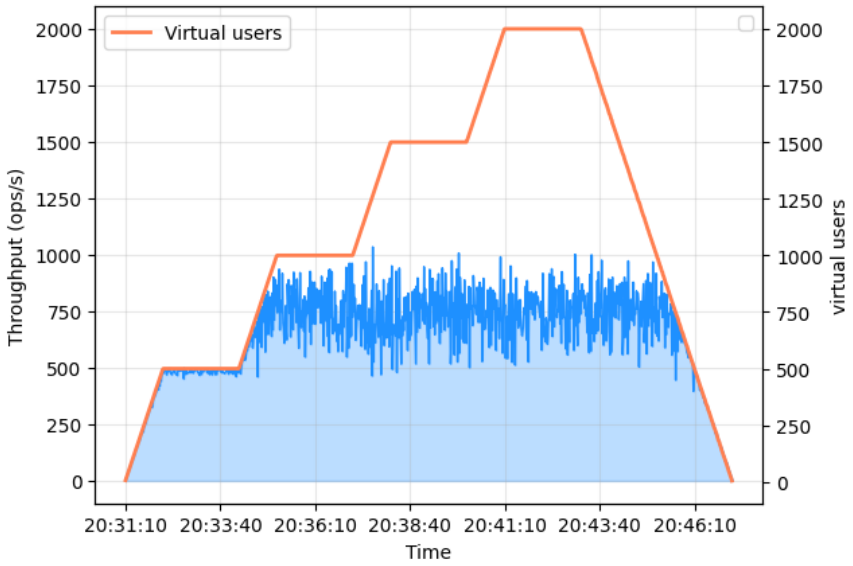


Figure 6.3: IoT Broker Throughput (GET Requests)

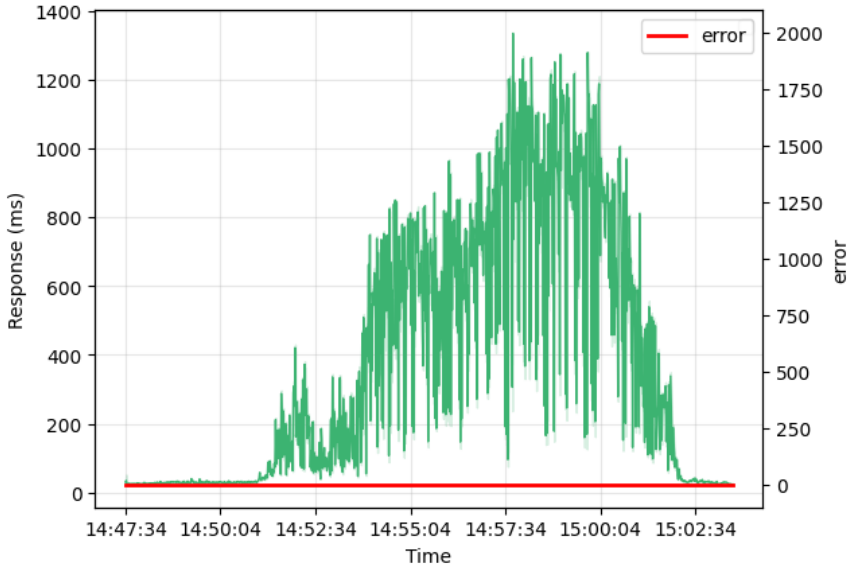


Figure 6.4: IoT Broker Response Time (POST Requests)

the response times for both types of requests also increase significantly, implying that the IoT Broker begins to struggle to handle heavier loads. As the load increased, the response time became increasingly variable, with higher peaks and greater fluctuations in the case of POST-type requests (Figure 6.4). In the case of GET-type requests (Figure 6.5), the response time also increased, but with low fluctuations. For both experiments, all the requests were completed without any errors.

6.1.2.2 BN Throughput

Once the operation of the elements from the testbed was verified and the chaincode was instantiated within the peers that make up the decentralized network,

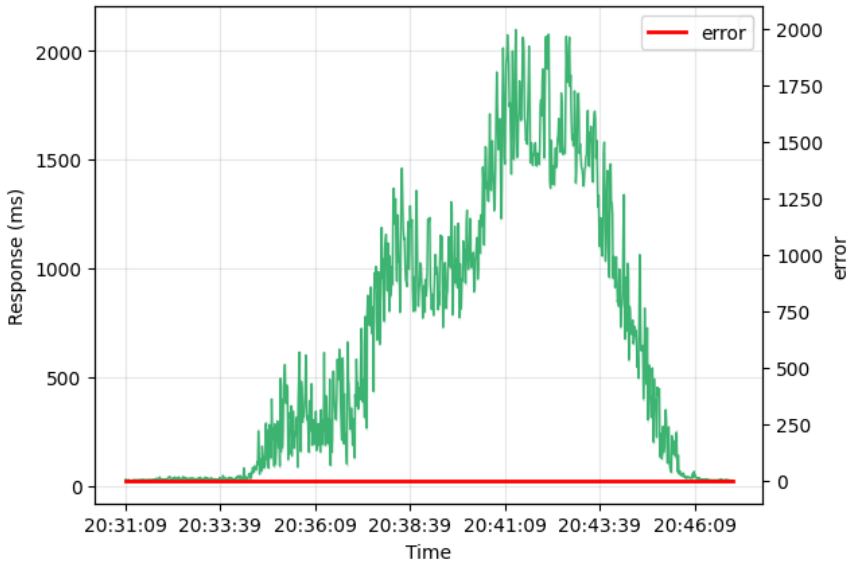


Figure 6.5: IoT Broker Response Time (GET Requests)

the first assessment metric was the throughput. This metric represents the number of successful transactions per second (TPS). To run this experiment, the network was subject to several bursts of TPS, starting with 25 TPS and reaching 350 TPS in the case of ledger-querying operations, and 300 TPS in ledger-updating operations. These transactions invoke the functions defined in the chaincode whose purpose is to write to or read into the ledger. Each of the bursts was executed 30 times and, based on the obtained data, the values for the average throughput (Ψ) were obtained, as shown in Figures 6.6 and 6.7. To run these experiments, a Hyperledger Caliper v0.4.2 container was used as a benchmarking tool.

In the case of ledger-querying operations (Figure 6.6), Ψ linearly grows up to 125 TPS bursts. After this point, a slight decrease of Ψ is observed, for bursts from 150 to 200 TPS. In the case of the transactional blocks from 225 to 250 TPS, it is observed that Ψ is close to 199 (Ψ_{MAX}) and 197 respectively. For higher burst rates, a drop of Ψ to a range between 141 and 129.4 is observed. In the case of the ledger-updating operation (Figure 6.7), Ψ is always lower than the values of the bursts, which means that the network was never able to write to the ledger the total number of TPS of each burst. For the first burst (25 TPS), Ψ= 22.5. Ψ_{MAX} is reached at the 125 TPS burst, with a throughput value of 42.7 TPS. From that point on, Ψ oscillates between 38.77 and 41.45 TPS.

6.1.2.3 BN Latency

The second metric to be assessed was latency, which represents the time interval elapsed between the transaction proposal and its execution. Based on the obtained data, the graphs of the average latency values (Γ) were drawn, as shown in Figures 6.8 and 6.9.

In the case of ledger-querying operations (Figure 6.8), Γ grows slightly during

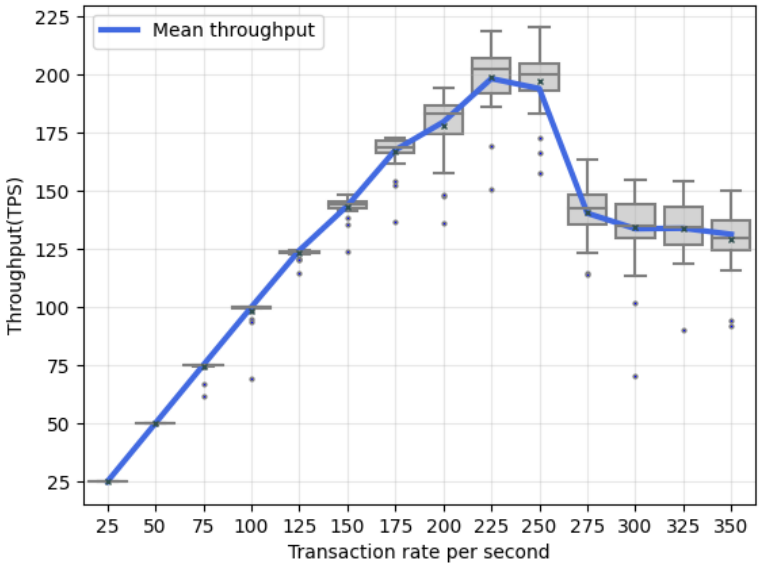


Figure 6.6: Average throughput for the case of ledger-querying operations

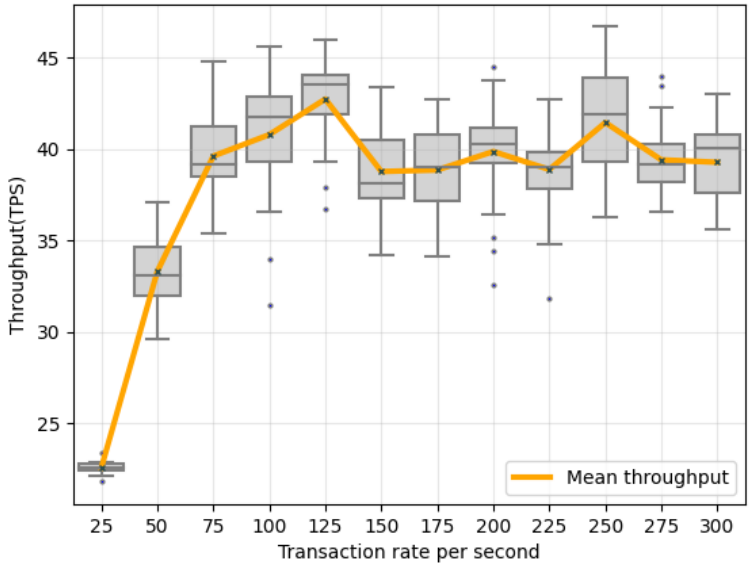


Figure 6.7: Average throughput for the case of ledger-updating operations

the first five transaction bursts, and keeps values that are always lower than 0.1 seconds. For the cases of burst values of 150 TPS to 300 TPS, Γ has a more accelerated growth, reaching a value of 0.8 seconds. From that point on, latency stabilizes at a value close to 0.85 seconds (input bursts of 325 and 350 TPS). For the case of ledger-updating operations (Figure 6.9), Γ starts at 1.37 seconds for the 25 TPS burst and grows to its maximum value $\Gamma_{MAX} = 3.89$ seconds, which is reached in the case of 225 TPS input burst. However, from the 150 TPS burst onwards, a mostly stable Γ value is observed, ranging from 3.60

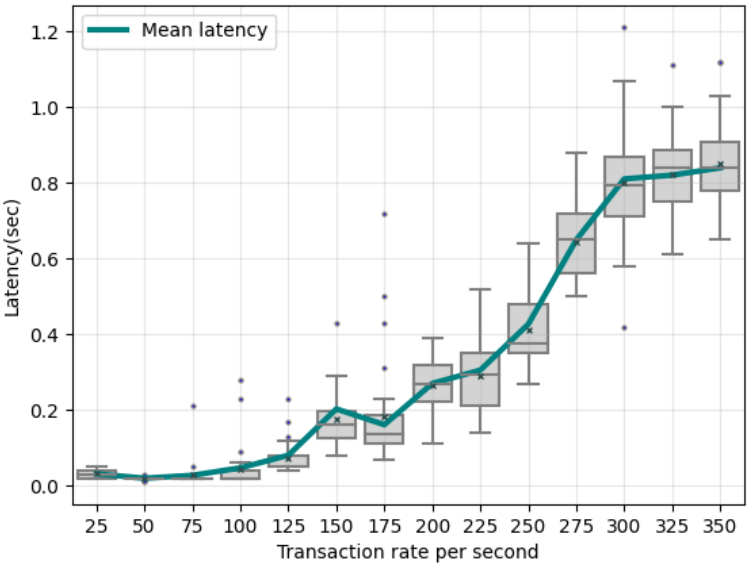


Figure 6.8: Average latency for the case of ledger-querying operations

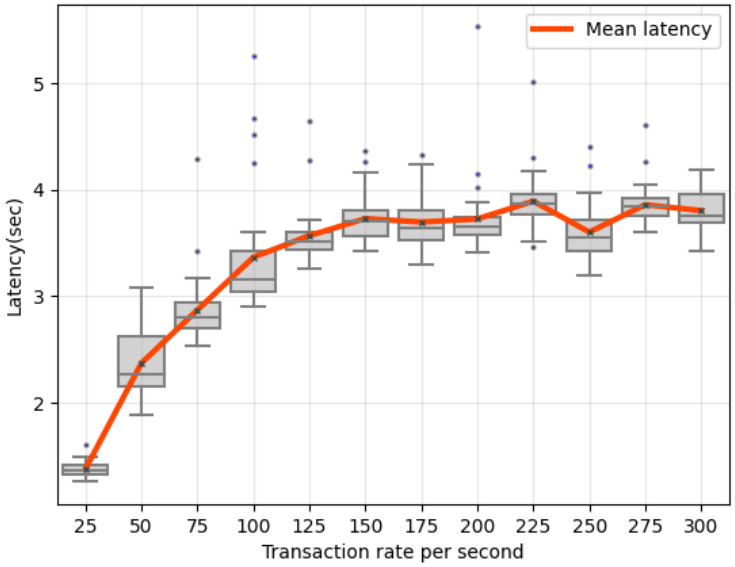


Figure 6.9: Average latency for the case of ledger-updating operations

seconds to 3.89 seconds. The difference between ledger-updating and ledger-querying latency mean values is due to the additional processes in the former case. For the ledger-querying case, the process is straightforward, since the peer only consults its local copy of the ledger to complete the operation. However, in a ledger-updating case, it relies upon the rest of the peers and the ordering service, and only after a consensus is reached the operation is complete.

6.1.2.4 Impact of the Proxy Re-encryption

Before delving into the details of the last set of experiments, it is important to further characterize the testbed. There are two data owners (DO_1 and DO_2). Both have selected a total of 30 IoT resources through their PPIs. The data from these resources is encrypted by the IoT Gateways and forwarded to the IoT Broker. The former has made these resources available to two DRs (DR_1 and DR_2). They have generated consent requests and the DOs have had the opportunity to decide whether to grant or deny those requests. Eighteen resources, among them accelerometer, compass, GPS, gyroscope, geospatial orientation sensor, ligth sensor, proximity sensor, sound sensor, device information(operating system, current app in foreground, battery level, network interfaces information), activity-recognition virtual sensor, have been granted by both DO, and thus the DRs can request the data from those resources to the IoT Broker.

This set of experiments was oriented to measure the impact of the re-encryption process. For these experiments, data access requests were generated to the IoT Broker, which is the custodian of the approved resource data. Resource data sizes range from 5.12KB to 76.56 KB. As in the first experimental stage (subsections 5.2.1 and 5.2.2), 30 requests were made for each resource, both for the scenario without the re-encryption process and for the one that includes this process. For each request, the time it takes for the IoT Broker to retrieve the requested resource data and the execution or non-execution of the re-encryption process was measured. From the 30 iterations per resource, the mean value in milliseconds was determined. The results of this experiment are presented in Figure 6.10.

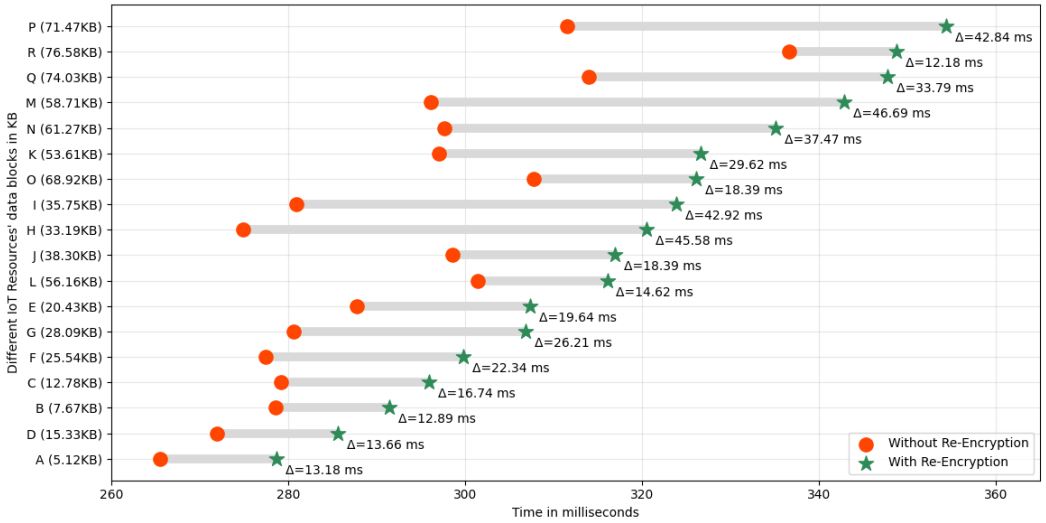


Figure 6.10: Impact in time of re-encryption process in the response time of a data release phase.

6.1.3 Second approach assessments

In this section, we describe the assessment to second approach of out model, related to the state inference of a HiTLCPS.

6.1.3.1 HiTL Service

For this evaluation we leveraged the Sleep Detection service provided by ISABELA [Fernandes et al., 2020]. This service infers whether the user is sleeping according to the data retrieved from smartphone sensors. As the smartphone cannot directly record a person's sleep, most studies use passively sensed data and user reports to detect sleeping behaviors and label the data used in the Machine Learning process [Kulkarni et al., 2022].

Sleep detection is a service that includes sensitive information such as location and microphone level. Because of these characteristics, we evaluate the generated models considering the traditional centric approach with the FL one. We aim to understand the performance impact to increase privacy protection. For that, we describe in the following three sections: (1) the description of different learning methods which we compare here; (2) the description of the data; (3) the experiment results and further discussions.

6.1.3.2 Used machine learning methods

The tradition ML and FL procedures involve distinct stages of interaction and model generation. To facilitate the depiction of the processes employed in our experiments to assess both models, we provide a visual representation in Figure 6.11. This illustration highlights local device activities in blue, communication activities in green, and server operations in red.

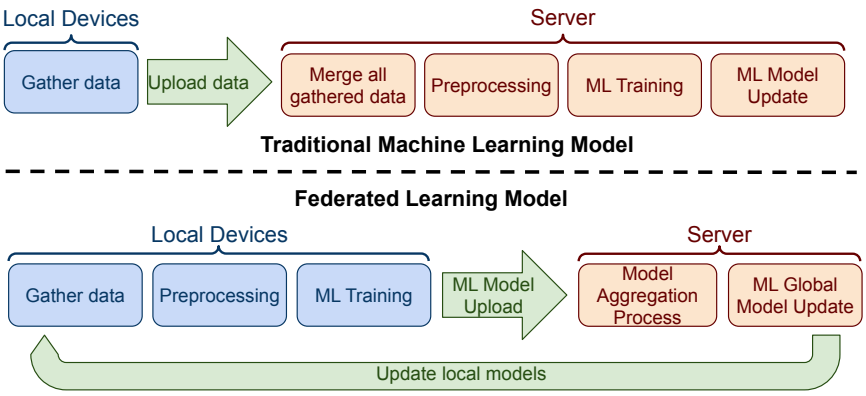


Figure 6.11: Processes of Machine Learning and Federated Learning performed on the experiments

The traditional ML model follows a procedure that commences with the compilation of data from all devices, which is then transmitted and stored within a central database on the server. Once the requisite data is gathered, it undergoes preprocessing to ready it for the generation of the ML model. Following

the model's creation, it can be dispatched to the devices. In our scenario, we employed the finalized model to assess our test dataset.

In contrast, the FL model employs an iterative learning approach where data remains on the respective devices. Consequently, all testing data remains partitioned by users. For each individual device, its data is utilized to train a distinct ML model, which is then dispatched to the server after generation. Subsequently, the server aggregates these models into a global model. This global model is then circulated to each user, initiating the process anew for every iteration. The ultimate model produced through these iterations is also subjected to testing using the same test dataset that was employed in the conventional ML model.

6.1.3.3 Data description and treatment

The dataset[1] was subject to treatment and preprocessing akin to the methodology employed in Fernandes et al. [2020]. The features utilized in our present case study are outlined in Table 6.3. Categorical attributes such as Location, Activity, Phone Lock, and Day of the Week were translated into numeric values ranging from 1 to N. Following preprocessing, all data underwent normalization for the ML process, ensuring values resided between 0 and 1. The output class is dichotomous, comprising "awake" and "asleep," which we transformed into two output neurons via one-hot encoding [Dahouda and Joe, 2021]. In the context of FL datasets, preprocessing transpires on each device, prompting the adoption of a fixed reference value for the normalization process across all local datasets. This value is also presented in Table 6.3.

Table 6.3: Dataset Features and Specifications

FEATURE	DATA DESCRIPTION	REFERENCE VALUE
Activity	Categorical values: Unknown, Still, Tilting, Exercise, In-vehicle	5
Location	Categorical values: Other, University, House	3
Day of the Week	Categorical values: Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, Monday	7
Phone Lock	Categorical values: not locked, locked	2
Sound amplitude	A numeric value between 0 and 32768	32768
Minutes_day	A numeric value between 0 and 1439 minutes (equivalent to 24hs)	1439
Time to Next Alarm	A numeric value between 0 and 604800000 milliseconds in a day (the equivalent of 7hs am)	604800000
Light intensity	A numeric value between 0 and 211880	211880
Proximity Sensor	A numerical value between 0 and 10 centimeters. We consider a binary value of 0 or 1 if the value is different from 0 because we only need information on whether the device is inside a container or not.	1

The dataset provided by Fernandes et al. [2020] encompasses information gathered from 30 users over a 4-week experimental period spanning from 11/05/2018 to 13/06/2018. However, for the analysis at hand, only 27 out of the 30 users were considered, as three users did not respond to the form utilized for data labeling. Once the data was labeled, the distribution of samples revealed 289,267 instances for the "awake" class and 118,184 instances for the "asleep" class. It's important to note that this dataset comprises diverse data from all 27 valid users.

However, several users were unable to share specific smartphone sensor data, leading to data heterogeneity. Among these restrictions, ten users refrained

[1]The dataset, following the anonymization process, is accessible on our public Kaggle repository: https://www.kaggle.com/dsv/5804700. The source code is available in our public GitHub repository: https://shorturl.at/efyB8.

from sharing light sensor data, while two users each withheld sound sensor and proximity sensor data. Additionally, two users did not set up the time for the next alarm, a parameter employed as a software sensor. Moreover, within the 965 recorded sleep period entries reported by users, certain abnormal sleep periods were identified, attributed to human errors. Specifically, there were 58 sleep periods lasting between 12 to 24 hours and 73 sleep periods exceeding 24 hours.

The dataset was then segregated into two distinct sets. The initial set served as the training dataset, encompassing data from 19 users, constituting 75% of the complete dataset. The second dataset, designated as the test dataset, incorporated data from nine users. In the context of the traditional approach, all data was amalgamated into a single dataset. Conversely, for the FL scenario, individual client datasets were processed autonomously to replicate the distributed environment. Despite the different data processing routes, the same testing dataset was utilized to compute metrics for all models. The assessment of results relied on established machine learning metrics, including Accuracy, Precision, Recall, and F1-Score (F-measure).

6.1.3.4 Experiment result and discussion

The experiment setup was performed considering two ML models: Multi-Layer Perceptron (MLP) [Pal and Mitra, 1992] and Long Short-Term Memory (LSTM) [Hochreiter and Schmidhuber, 1997]. Both ML models were opted for, as they showcased over 90% accuracy in identifying sleep periods as affirmed by Kulkarni et al. [2022]. Furthermore, they align with the Neural Network-based models compatible with the FedAvg Algorithm [McMahan et al., 2017], the default FL aggregation process in TensorFlow Federated[2]. The MLP configuration entailed two hidden layers employing Rectified Linear Unit (ReLU) activation. On the other hand, LSTM operated via a unidirectional model, employing 2-minute epochs for sleep/wake state detection, encompassing input data sequences of 4 instances. Both models utilize the Softmax activation function to categorize the output layer into two outputs.

Regarding the traditional approach, 30 epochs were configured for MLP, and 50 for LSTM. This choice was prompted by the observation that accuracy ceased to increase beyond these epochs. Notably, as the FL approach attains superior results with fewer epochs compared to the traditional approach, this study employed 10 epochs across 13 rounds for LSTM and 3 epochs throughout 9 rounds for MLP. After each round, the FedAvg Algorithm was executed to merge models from all 19 training clients into a global model [McMahan et al., 2017].

The comparison between traditional ML and FL outcomes is visualized in Figure 6.12, in the case of MLP, and in Figure 6.13 in the case of LSTM. This results are also summarized in Table 6.4. Notably, both MLP and LSTM are sensitive to the unbalanced dataset, where instances from the awake class outnumbered

[2]https://www.tensorflow.org/federated

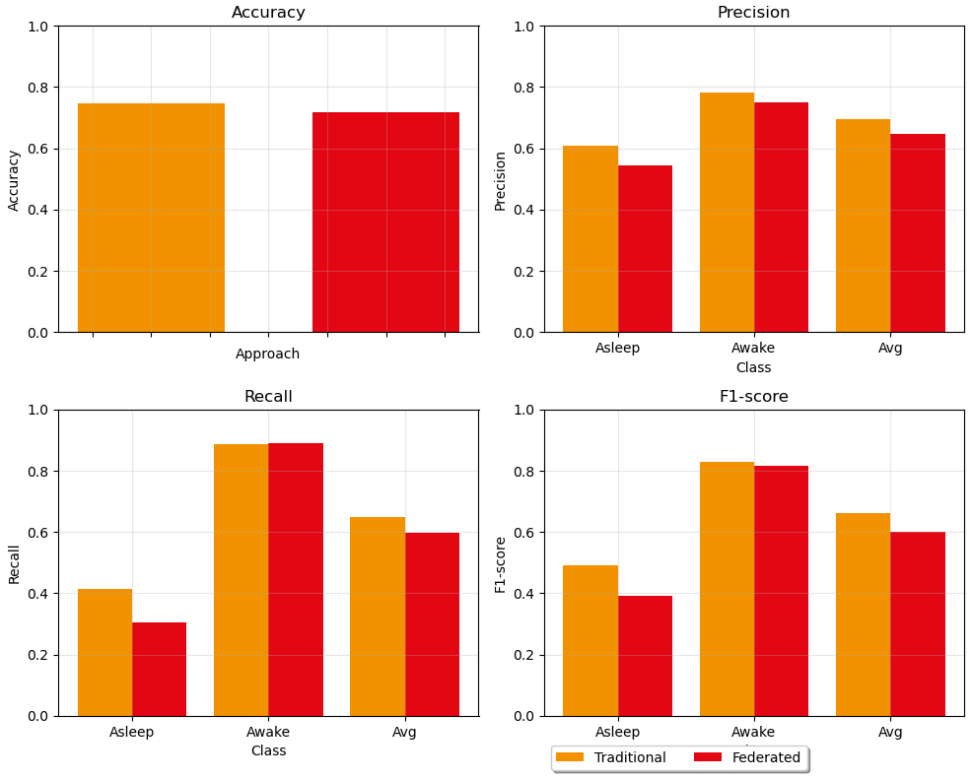


Figure 6.12: Results from traditional ML and FL models approach using MLP

those from the asleep class by approximately 2.44 times. This imbalance is more pronounced in Precision, F1-scores, and Recall metrics compared to Accuracy. Nevertheless, it is noteworthy that across all ML classifiers, the traditional approach consistently outperformed the FL variants across all metrics, albeit by a minor margin (averaging an absolute 0.025 accuracy discrepancy or 3.27% relative accuracy improvement). This implies that the accuracy trade-off for enhanced privacy protection in our application remains negligible.

However, when evaluating metrics such as precision, recall, and F1-score, the MLP exhibited an average reduction of 18.16% in its values within the federated solution compared to the traditional approach concerning the minority class: asleep. This divergence primarily stemmed from the fact that the variability in data from each user found more robust representation in a learning model that utilized the entire training set as a whole. This distinction is manifest in the overall improved average values as detailed in Table 6.4.

Furthermore, some users refrained from sharing certain device data or reported abnormal information in their submissions. As a consequence, the quality of data was compromised, subsequently influencing the aggregation process carried out by the FedAvg Algorithm [McMahan et al., 2017] and, consequently, the generalization process. These challenges arising from localized data irregularities are topics to research in future works.

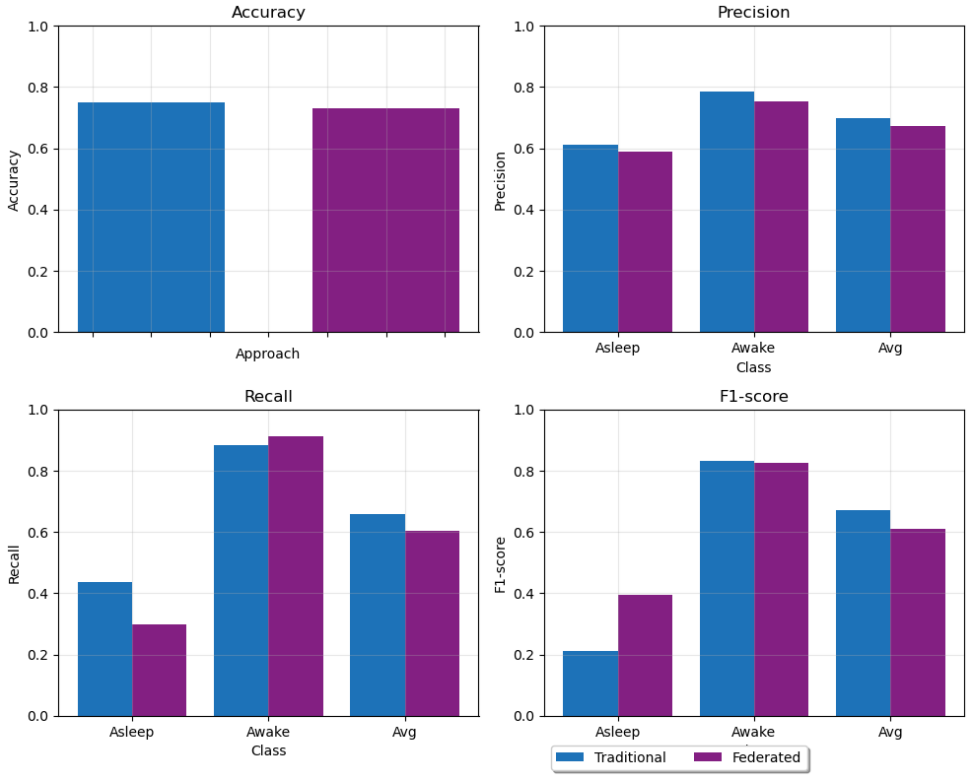


Figure 6.13: Results from traditional ML and FL models approach using LSTM

Table 6.4: Values between ML and FL models Experiments

CLASSIFIER	APPROACH	ACCURACY	CLASS	PRECISION	RECALL	F1-SCORE
MLP	Traditional	0.746	Asleep	0.608	0.413	0.492
			Awake	0.781	0.887	0.830
			Avg	0.694	0.650	0.661
LSTM	Traditional	0.749	Asleep	0.611	0.436	0.212
			Awake	0.786	0.883	0.831
			Avg	0.698	0.659	0.670
MLP	Federated	0.716	Asleep	0.543	0.305	0.390
			Awake	0.751	0.891	0.815
			Avg	0.647	0.598	0.602
LSTM	Federated	0.730	Asleep	0.589	0.299	0.396
			Awake	0.753	0.912	0.825
			Avg	0.671	0.605	0.611

6.2 Integration Model

Once the implementation of the elements defined by our model is described, the next step is to integrate each element into a PoC to assess the viability of our proposal. Therefore, this section is divided into two parts: the first part describes the testbed architecture for this PoC, and the second part presents the results of a set of tests executed over the prototype platform.

6.2.1 Prototype Platform Deployment - Test Environment

For the deployment of this prototype, a scenario composed of the entities of the model was defined, and virtual instances and physical devices were used to

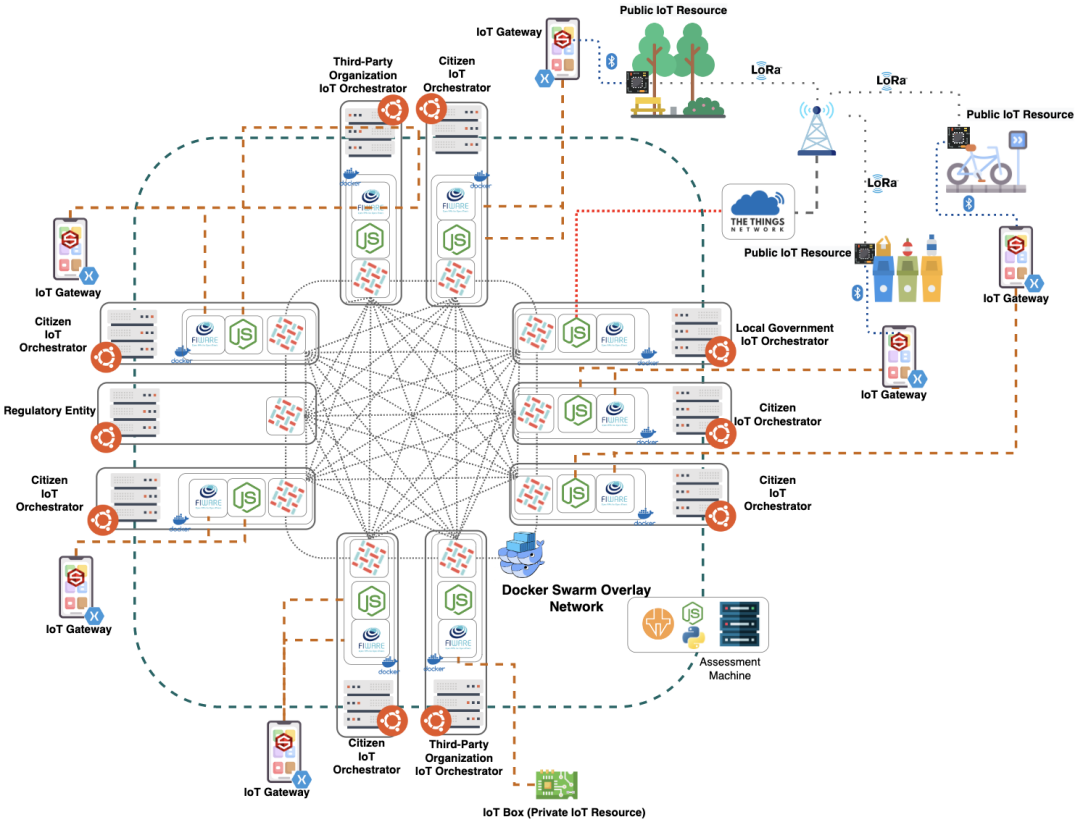


Figure 6.14: SPACES Testbed for the CONFLUENCE model

represent each component, as illustrated in Figure 6.14. With respect to the entities, the scenario included one local government, two third-party organizations, six citizens, and one regulatory entity. The technological infrastructure of each of these entities is represented by a virtual machine deployed within our institutional cloud. Each of these virtual instances forms an IoT Orchestrator, which includes a corresponding node of the blockchain network, with the exception of the VM of the regulatory entity, which only implements the node of the decentralized network. These nodes integrate an overlay network based on Docker Swarm and fulfill the functions of peers and, in turn, are part of the ordering service defined by HLF.

In the case of IoT resources, the local government manages three physical devices deployed in different parts of the city. In the case of third-party organizations, one of the organizations manages the IoT Box. On the other hand, mobile devices have been used to perform the functions of the IoT Gateway; therefore, sensors from these devices are also part of the IoT resource pool.

Finally, an additional virtual instance was used for benchmarking purposes and running tests on the components. The technical specifications of the virtual instances as well as the devices used are summarized in Table 6.5.

Table 6.5: Technical specifications testbed platform components

Components	**CPU**	**RAM**	**OS**
Local Government IoT Orchestrator	Intel(R) Xeon(R) E5-2650 v42 x 2.20GHz	6 GB	Ubuntu 20.04.5 LTS
Citizen IoT Orchestrator	Intel(R) Xeon(R) E5-2650 v4 2 x 2.20GHz	3 GB	Ubuntu 20.04.5 LTS
Organizations IoT Orchestrator	Intel(R) Xeon(R) E5-2650 v4 2 x 2.20GHz	4.5 GB	Ubuntu 20.04.5 LTS
IoT Gateway 1	A10 Fusion 4 x 2.34 GHz	2 GB	iOS 15.5
IoT Gateway 2	HiSilicon Kirin 659 Cortex-A53 4 x 2.36 GHz	4 GB	Android 8
IoT Gateway 3	A15 Bionic 6 x 2.34 GHz	4 GB	iOS 16.3
IoT Gateway 4	Snapdragon 855 Qualcomm 1x 2.84 GHz Kryo 485 3x 2.42 GHz Kryo 485 4x 1.8 GHz Kryo 485	6 GB	Android 11
IoT Gateway 5	Snapdragon 450 Qualcomm 8 x 1.8 GHz	3 GB	Android 8.1
IoT Gateway 6	4x 2.45 GHz Kryo 280 4x 1.9 GHz Kryo 280	6 GB	Android 10
Assessment VM	Intel(R) Xeon(R) E5-2650 v4 4 x 2.20GHz	4 GB	Ubuntu 20.04.5 LTS

6.2.2 Assessment

The actions triggered by the interactions between entities and components during the processes related to data sharing (registration of IoT services and DR profiles, exchange of privacy policies, consent management, and data access), as well as those associated with the incentive mechanism, are closely related to the actions to be executed on the blockchain. Based on this premise, the first part of the evaluation focused on determining the network throughput and latency. The first metric identifies the number of transactions that can be processed by the network in different time periods, while the second metric is the time the network takes to process a set of transactions. To generate the workloads, the experiment used Hyperledger Caliper 0.5.0 as a benchmarking artifact. The second part of the assessment was oriented toward the communication aspects of public IoT resources.

6.2.2.1 Throughput

Two scenarios are considered in the evaluation of this metric. The first corresponds to a network in which the proposed transactions have the objective of executing ledger-updating operations, whereas the second scenario corresponds to transactions involving only ledger-querying operations. In both cases, the network was subjected to a set of bursts of TPS, starting with 20 TPS and up to 400 TPS in a fixed-interval of 20 TPS. These transactions aim to invoke write (in the case of ledger updating) and read (in the case of ledger querying) functions defined within a chaincode that was previously instantiated in the network nodes. Each burst was executed 30 times, and the average throughput (Ψ) was obtained from the data.

As shown in Figure 6.15, the value of Ψ does not approach the value of the transaction rate of each burst, except for the first burst, where the average value is 19.56 TPS. This means that as the transaction rate increases, the network cannot execute the ledger-updating operation in one second. Ψ_{MAX} is reached in the eleventh burst, with an average throughput of 37.14 TPS. Similarly, it can be observed that from the third burst onwards the value of Ψ oscillates between 33.8 and 36.5 TPS, with the notable exception of bursts 280, 300, 380, and 400 TPS where the average value is below this lower limit. In the case of penultimate burst, a significant decrease to an average throughput value of 22.48 TPS is observed.

In the case of ledger-querying operations (Figure 6.16), linear growth is observed up to 240 TPS, which means that the network has been able to process all transactions of each of these bursts. A slight decrease in Ψ is observed in the subsequent three bursts. However, from 320 TPS onwards, the value of Ψ does not drop bellow 290 TPS and reaches a maximum average value of 311.50 TPS in the penultimate burst.

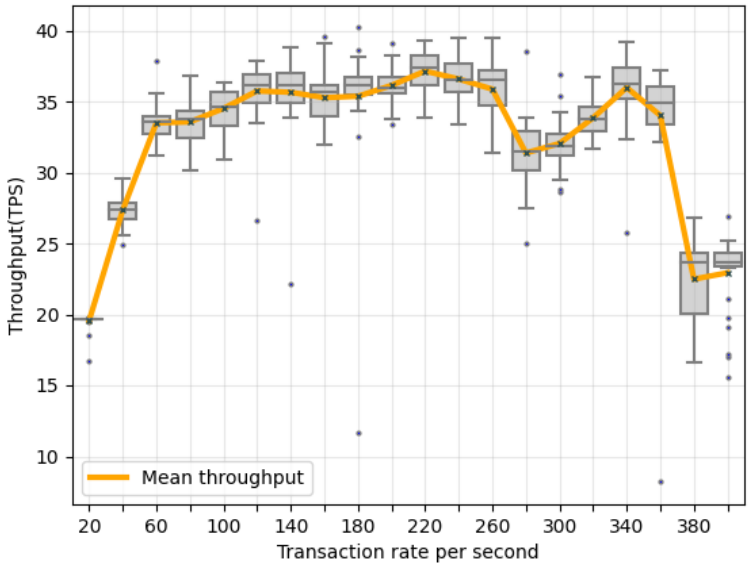


Figure 6.15: Average throughput for the case of a ledger-updating operation

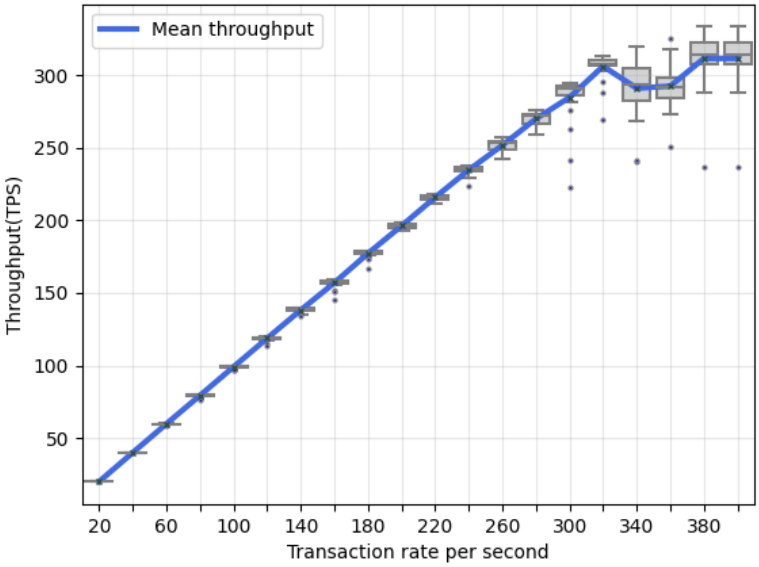


Figure 6.16: Average throughput for the case of a ledger-querying operation

6.2.2.2 Latency

As in the case of throughput, the second experiment aimed to determine the average latency (Γ) for both the scenarios. This metric represents the time interval between the proposal and execution of a transaction. Figures 6.17 and 6.18 show this metric for both the cases.

For transactions involving ledger-invoking operations (Figure 6.17), Γ starts with a mean value of less than one second during the first burst. When the transaction

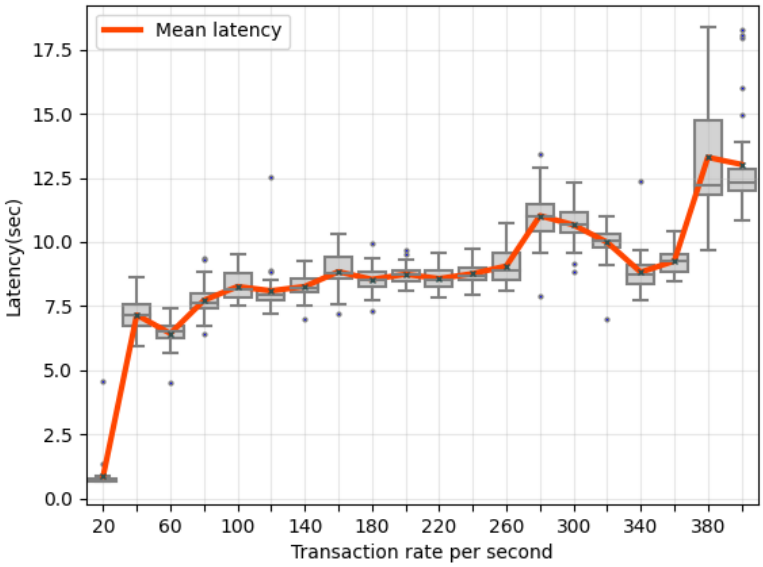


Figure 6.17: Average latency for the case of a ledger-updating operation

rate reaches 40 TPS, the latency suddenly increases on average to 7.16 seconds; however, a small decrease is observed at the 60 TPS burst. Between the 80 and 260 TPS bursts the value of Γ ranges from 7.7 seconds to 9.1 seconds. As expected, when the transaction rate was 280 TPS, the latency increased by 21.6%, which is related to what was observed during the first experiment, where the throughput decreased considerably. For the next three bursts, the value of Γ decreased slightly, and it was not until the 380 TPS rate that Γ reached its maximum value (Γ_{MAX}) of 13.29 seconds. In the case of transactions that trigger ledger-query operations (Figure 6.18), Γ remains below 0.06 seconds until 280 TPS and increases in the next burst to 0.107 seconds. From then on and during the next three bursts, Γ oscillated between that value and 0.07 seconds. Γ_{MAX} was reached at 380 TPS (0.144 s).

6.2.2.3 Public IoT resources in a TTN Network

The interactions carried out by the entities within a platform directly impact the execution of actions within the blockchain. Therefore, this section evaluates the public IoT resources, devices or nodes utilized, and the public TTN platform that interacts with the local government's IoT orchestrator.

The assessment was conducted in Coimbra, Portugal, based on the general architecture of the "Green Bear" [Sanchez et al., 2022] case study, which utilizes LoRaWAN for sustainable cities. This architecture leverages the infrastructure and public LoRaWAN gateway distribution offered by TheThingsNetwork to communicate via LoRaWAN using Pycom nodes. Moreover, the "Green Bear" 3-byte frame was used as the foundation, where 2 bytes are allocated to communicate the user pseudo identifier, 5 bits to identify the node activity, and 3 bits to sub-identify the node functionality.

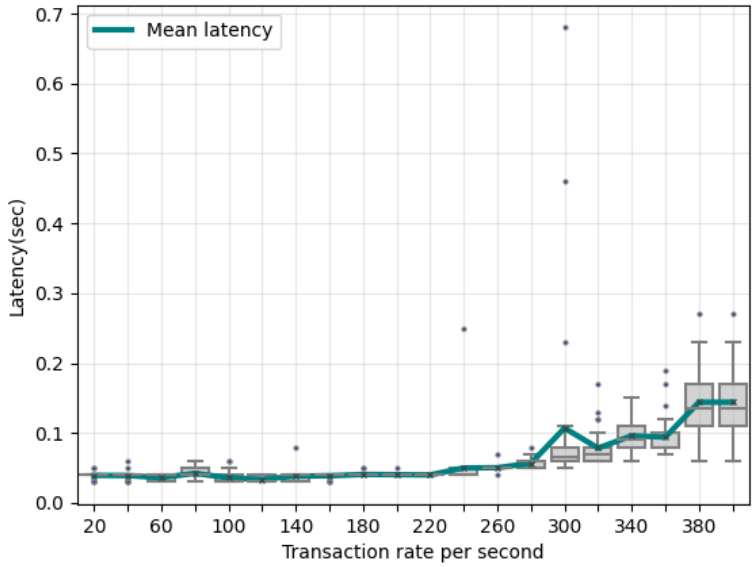


Figure 6.18: Average latency for the case of a ledger-querying operation

This section presents insights into the quality of communication between public IoT resources and LoRaWAN gateways, specifically focusing on the predefined distribution of devices in spaces of interest to public entities. The assessment of LoRaWAN gateway performance in terms of their capacity to process pseudo-identifiers and achieve optimal signal quality is of paramount importance, as it enables informed decision-making in terms of device placement within the solution prior to integration with the blockchain network. By identifying LoRaWAN gateways that exhibit higher processing capabilities and superior signal quality, public entities can effectively manage the positioning of devices, thereby optimizing the overall performance and reliability of the LoRaWAN communication network.

To conduct the tests, we positioned three nodes in different locations around the city of Coimbra, as detailed in Table 6.6. Furthermore, we performed coverage tests to discover which LoRaWAN gateway the nodes can communicate with considering a modulation SF7; those LoRaWAN gateways are also specified in Table 6.6. The LoRaWAN gateways' distribution, as shown in Table 6.7, was taken into account, and we will henceforth refer to the numbers presented in that table. Figure 6.19 visually represents the distribution of nodes and LoRaWAN gateways used for these tests. We deliberately selected green spaces where public entities, such as the City Council of Coimbra, could implement this system.

The experiments entailed progressively generating user load to be transmitted by each node. We considered the restrictions imposed by the number of bytes allowed per message, as outlined in Sanchez et al. [2022], which specifies a maximum of 74 identifiers per frame. Consequently, the nodes progressively transmitted frames ranging from 1 to 74 identifiers to test various scenarios and message sizes. The testing took place over 21 days, during which the nodes trans-

Table 6.6: Devices, coordinates and LoRaWAN gateways that receives frames from each node

Node	**Coordinates**	**LoRaWAN Gateways**
Node 1	Latitude: 40.186702 Longitude: -8.415076	eui-647fdafffe00577c eui-fcc23dfffe0ddccb eui-fcc23dfffe0efabb
Node 2	Latitude: 40.219295 Longitude: -8.4367507	eui-647fdafffe00577c eui-647fdafffe0057a0-1 eui-647fdafffe00c66d eui-fcc23dfffe0dbc0a eui-fcc23dfffe0ddccb eui-fcc23dfffe0efabb eui-fcc23dfffe2ea900 eui-fcc23dfffe2eb0f0
Node 3	Latitude: 40.190836 Longitude: -8.406120	eui-647fdafffe00577c eui-647fdafffe0057a0-1 eui-fcc23dfffe0dd4e8 eui-fcc23dfffe0ddccb eui-fcc23dfffe2ea900 eui-fcc23dfffe2eb0f0

Table 6.7: Public LoRaWAN Gateways information

Ref	**LoRaWAN Gateway ID**	**Coordinates**
1	eui-647fdafffe00577c	Latitude: 40.1954487 Longitude: -8.4038303
2	eui-647fdafffe0057a0-1	Latitude: 40.21766 Longitude: -8.405659
3	eui-647fdafffe00c66d	No GPS information
4	eui-fcc23dfffe0dbc0a	No GPS information
5	eui-fcc23dfffe0dd4e8	Latitude: 40.192282 Longitude: -8.411066
6	eui-fcc23dfffe0ddccb	Latitude: 40.205111 Longitude:-8.41559
7	eui-fcc23dfffe0efabb	Latitude: 40.186861 Longitude: -8.417793
8	eui-fcc23dfffe2ea900	Latitude: 40.21135 Longitude: -8.42898
9	eui-fcc23dfffe2eb0f0	Latitude: 40.20702 Longitude: -8.42443

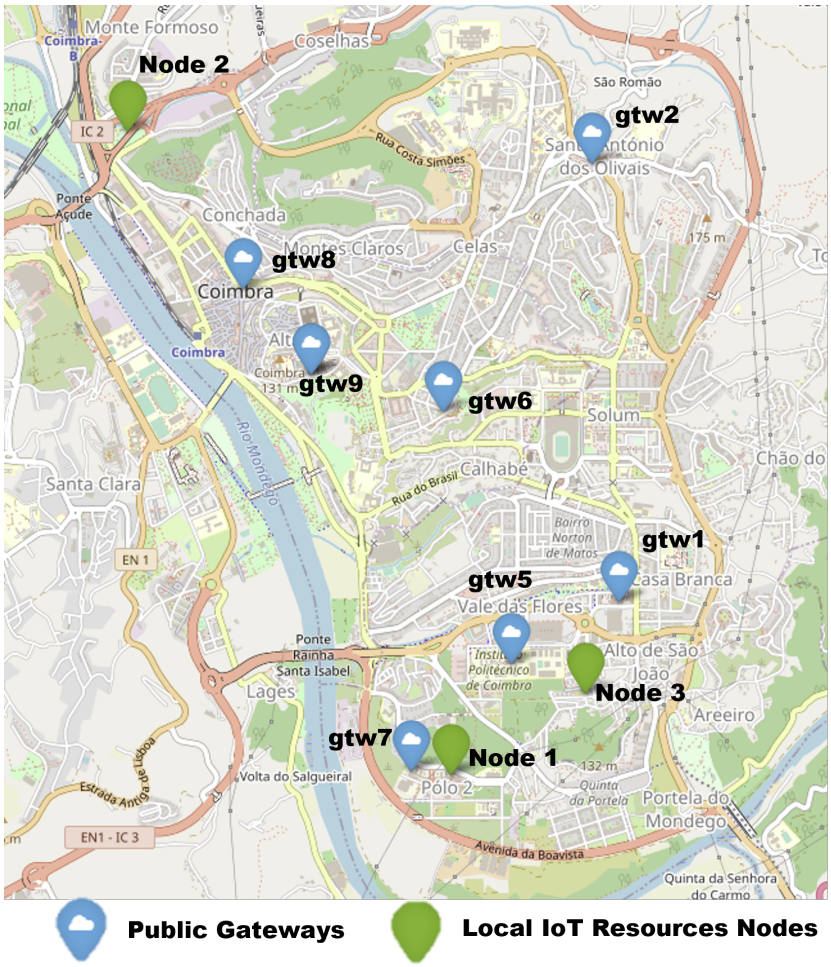


Figure 6.19: Map Distribution of IoT resources nodes and public LoRaWAN gateways

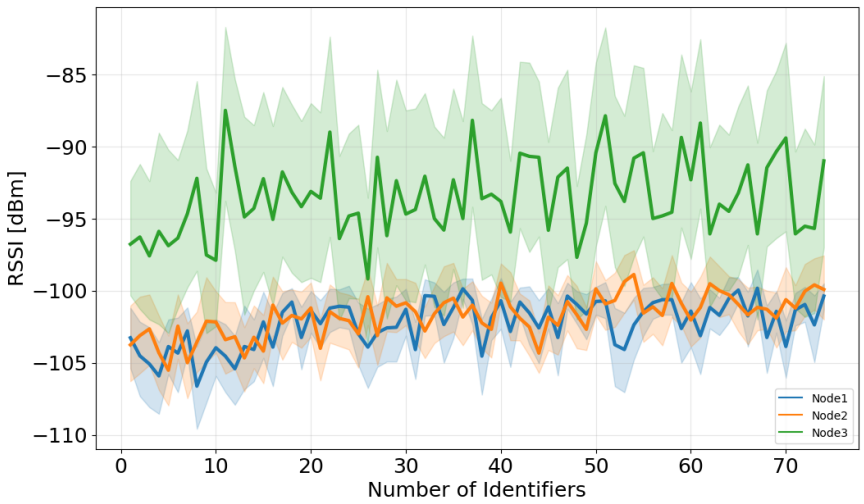


Figure 6.20: Mean of RSSI for each number of identifier

mitted the progressive uploads at different intervals, ranging from 10 seconds to 600 seconds.

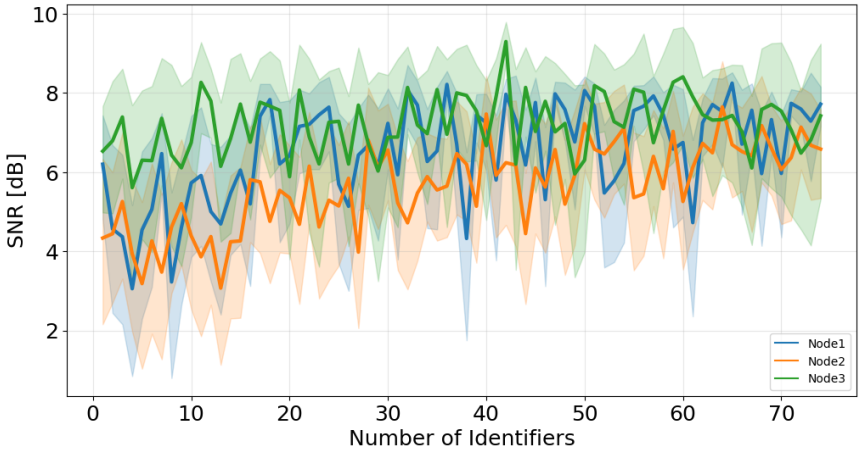


Figure 6.21: Mean of SNR for each number of identifier

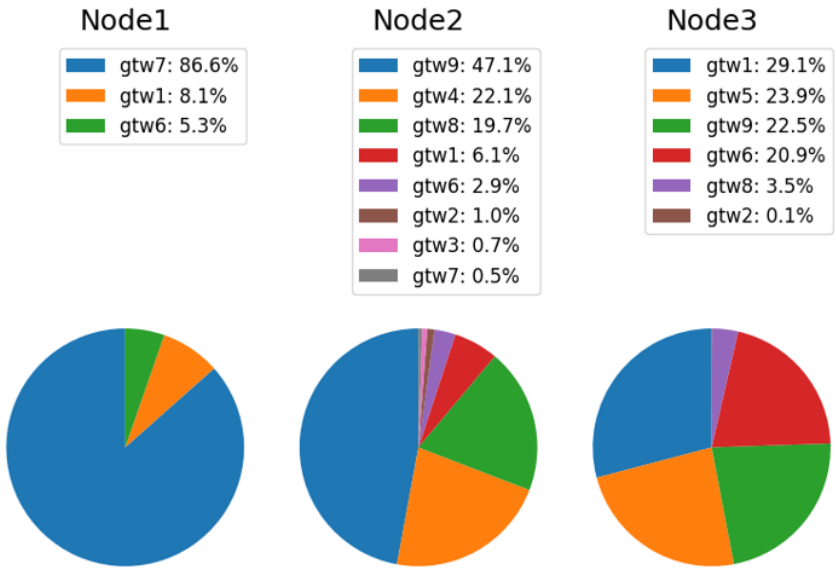


Figure 6.22: Percentage Frames per LoRaWAN Gateway

Figure 6.20 presents the average Received Signal Strength Indicator (RSSI) measured for each number of identifiers transmitted by the nodes. Node 3 exhibits the best location and LoRaWAN gateway access communication quality, whereas nodes 1 and 2 have comparable communication quality. These results raise the possibility of enhancing the location of the first node since it is near a LoRaWAN gateway, yet the average RSSI is relatively low. Moreover, a moderate improvement in the communication quality of the nodes is observable as the number of identifiers increases, indicating that it is preferable to maintain the users at the maximum before communicating with the TTN servers. This observation is reinforced by the Signal-to-Noise Ratio (SNR) of each node, as shown in Figure 6.21, which becomes more consistent between each node when the messages reach the maximum number of transmitted identifiers, reaching as high as 7 or 8 dB.

In this evaluation, great importance was given to the involvement of TTN gate-

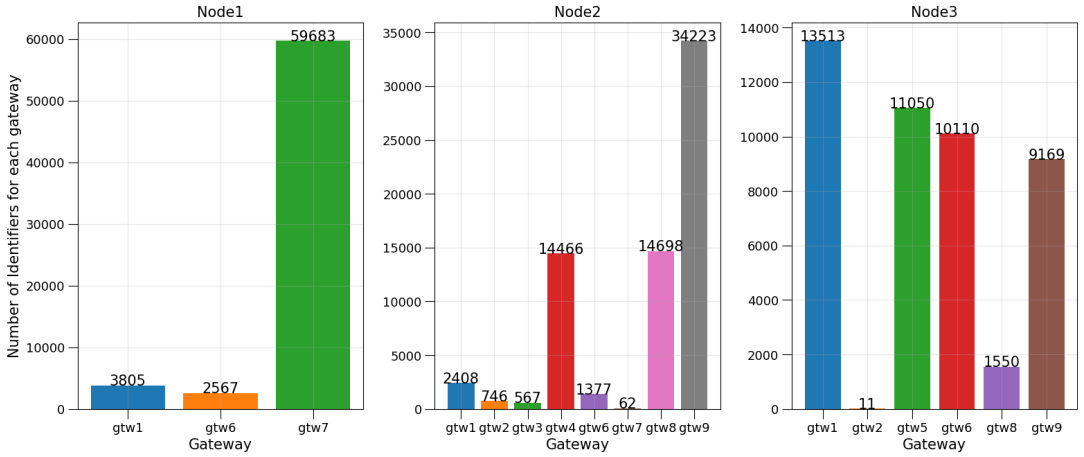


Figure 6.23: Number of identifiers per LoRaWAN gateway

ways and the communication of the nodes. Figure 6.22 shows the percentage of frames processed by each LoRaWAN gateway. In the case of node 1, the frames were mostly received by LoRaWAN gateway 7, located at the University of Coimbra. For node 2, despite its proximity to LoRaWAN gateway 8, the highest percentage of frames was processed by LoRaWAN gateway 9, also belonging to the University of Coimbra. LoRaWAN Gateway 8, located in the municipality of Coimbra, requires improvement in its antenna height or gain. For node 3, the highest percentage of frames was processed by LoRaWAN gateway 1, which is unsuitable for public solutions as it belongs to a private entity that could modify the LoRaWAN gateway's working conditions.

In this study, a crucial aspect to consider is the number of identifiers processed by each LoRaWAN gateway during the tests. To analyze this aspect, we progressively increase the number of identifiers sent by the nodes. It is worth noting that the capacity of the LoRaWAN gateways to receive larger frames can affect the number of identifiers in their limited frame size. In this context, Figure 6.23 illustrates the number of identifiers processed by each LoRaWAN gateway, providing insights into their ability to receive larger frames compared to other LoRaWAN gateways.

Moreover, as pointed out in a previous study Attia et al. [2019], the probability of successful packet reception is affected by environmental noise and collisions and the effective acquisition of the packet preamble, which represents the limiting factor. Our results support this finding, as we observed that some LoRaWAN gateways were more prone to receive larger frames. In contrast, others were more suitable for smaller ones, resulting in variations in the number of identifiers processed by each LoRaWAN gateway.

In addition to analyzing the capacity of LoRaWAN gateways to process identifiers, the quality of communication for each LoRaWAN gateway was also considered in this study. As expected, Figure 6.24 shows that nodes one and three exhibit higher average RSSI values for certain LoRaWAN gateways. However, for the second node, it is noteworthy that the ninth LoRaWAN gateway processes the highest number of identifiers despite not having the highest average

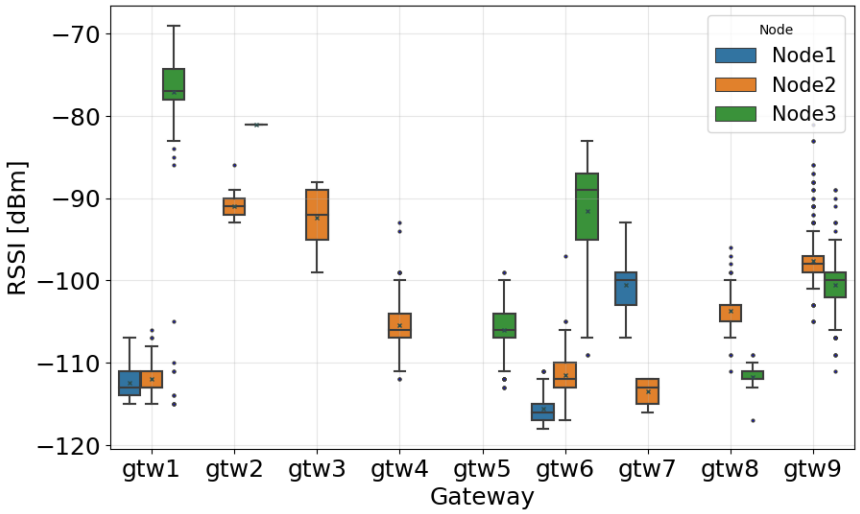


Figure 6.24: RSSI per LoRaWAN gateway and node

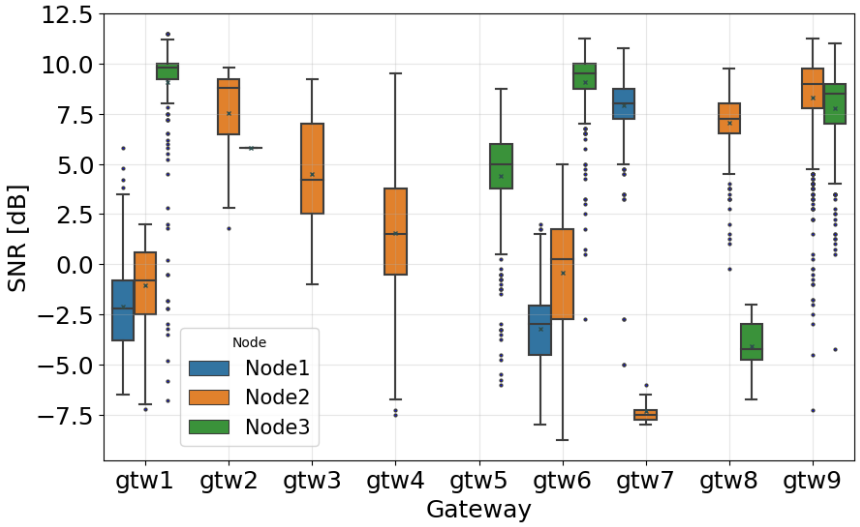


Figure 6.25: SNR per LoRaWAN gateway and node

RSSI—LoRaWAN gateways two and three exhibit higher average RSSI values. Furthermore, when comparing the fifth and the sixth LoRaWAN gateways, it is observed that the number of identifiers processed is similar, but the average RSSI values vary considerably. This suggests that nodes may prefer to communicate with LoRaWAN gateways that provide a stronger signal or faster processing on the server side. This leads to a diverse range of LoRaWAN gateways used in the communication process by certain nodes.

Additionally, when examining the SNR, a higher correlation is observed between the number of messages or identifiers processed by a LoRaWAN gateway and the average SNR value for that LoRaWAN gateway. This is evident in Figure 6.25, where all the nodes exhibit the highest SNR values in LoRaWAN gateways that process many messages and identifiers. This suggests that the volume of messages or identifiers in the SNR influences the performance of a LoRaWAN gateway.

The evaluation of this system primarily focused on assessing its performance based on parameters such as throughput, latency, and the evaluation of public IoT resources. These evaluations were conducted through controlled tests involving participating researchers and peers and analyzing the system's usage in the specified locations. The objective of these evaluations was to ensure that the system is well-prepared and tested for future implementation with natural communities, specifically to evaluate the sustainability aspects of the model. Subsequent phases of the project will encompass the evaluation of environmental, social, and economic metrics through prototypes and pilot projects. Key aspects to be analyzed include measuring the impact on the city's recycling practices through the system's interaction and assessing the utilization of green spaces. These data will provide the Municipality of Coimbra with valuable insights to evaluate the feasibility of scaling up the project. From a social perspective, future implementations will prioritize citizen engagement as a crucial element. The commitment and enthusiasm with which citizens receive these initiatives will be assessed, along with the accessibility of the services to ensure widespread usage among the majority of Coimbra's population. The central aim is to enhance the well-being of citizens, fostering healthier, active, and participatory engagement in the city's green activities.

Moreover, the economic dimension will be addressed in the upcoming project phases. The feasibility of public and third-party IoT resources will be evaluated alongside the cost of implementing the application for a community of approximately 150,000 inhabitants. The participation data will also highlight the interest of private entities in engaging with the community incentive system, further enhancing the system's dynamics.

In summary, the evaluation of the system initially was focused on performance aspects, and future phases will encompass comprehensive assessments of the environmental, social, and economic dimensions. These evaluations will provide valuable insights to support decision-making, assess feasibility, and optimize the system's sustainability per the Municipality of Coimbra's objectives.

6.3 Trust Perception in IoT Mobile Applications

ISABELA, Green Bear, and currently SPACES share a common ground. All these platforms aim to implement the concept of HiTLCPS by leveraging mobile applications and the convenience of smartphones, which have become indispensable personal devices in our daily lives. These applications, besides serving as means of interaction, also act as data generators based on inputs from internal sensors or other applications, such as social networks or native operating system applications. We will refer to them as IoT mobile applications. To apprehend the trust perception from DOs in this kind of applications, we will carry out a qualitative assessment.

Table 6.8: Participants Information

Participant	Academic Background	Age	Country
P1	Biomedical Engineering	28	Portugal
P2	High School	28	Portugal
P3	Physiotherapy	34	Portugal
P4	Design	28	Portugal
P5	Design and Computer Science	28	Portugal
P6	Social Communications Marketing	29	Portugal
P7	Business Administration and Computer Science	30	Ecuador
P8	Civil Engineering	23	Ecuador
P9	Mechanic Engineering	20	Ecuador
P10	Electronic Engineering	24	Ecuador
P11	Electronic Engineering	25	Ecuador

6.3.1 Participants and Interviews

We conducted semi-structured interviews with eleven participants to understand their perception of trust regarding IoT mobile applications. The age of the participants who collaborated with the research was between 20 and 34 years old, and their backgrounds are diverse as shown in Table 6.8. We believe it is relevant to mention that, unlike quantitative research, the number of subjects is handled differently in a qualitative approach. Thus, the sampling procedure is not limited to a predetermined number of interviews, but rather a model saturation. In a short, new interviews and/or observations are performed until all categories are saturated or in other words, when the research has discovered all emerging categories and their interaction [Lejeune, 2019].

The length of the interviews ranged from 9 to 15 minutes and all the interviews were recorded: six of them were face-to-face while the rest were conducted using video-conference. The interviewers initially provided context to the participants but without a prior introduction to the study objective, since we did not want to introduce possible bias. Some participants asked the purpose of the questions which was explained after the end of the dialogue.

In these conversations, users were asked the following: i) how and what type of information they feel mobile applications collect from them; ii) what type of information users usually would share with this kind of applications; iii) what type of information service providers could infer; iv) what type of protection providers could give to the data they collect and possible infer; v) what were their concerns regarding data sharing; vi) how they think companies use shared information; and vii) if they let applications retrieve more information for improving user-experience and why. The interview was conducted in the form of a

natural discussion with the participants and, at the end, the interviewer asked if the participant wanted to add some comment or express something that might have forgotten.

6.3.2 Qualitative Method Selection

For a proper interview processing, the first step was to transcribe the audio recordings. Then, through open coding [Salinger et al., 2008], all the answers obtained by the participants were reviewed and labeled with short phrases or terms. Those terms were the basis for the categories definition. After the definition, we built a model depicting the relationship between each of the categories. It is worth mentioning that this qualitative study is framed within Grounded Theory and the procedure of data analysis was based on Emerging Design [Miller and Salkind, 2002] which is less subject to predefined categories, and where the theory arises from the empirical data rather than from a set of prefixed categories as is the case with axial coding. In this design, the theory and model arise from the connection or relationship of the different emerging categories.

6.3.3 Interview insights

With the analysis of the interviews, we obtained a model concerning the perception of trust on mobile applications, as presented in Figure 6.26. We can see that Perception of Trust is directly influenced by three main factors: *Privacy Awareness*, *Perception of Information Exploitation* and the *Degree of Development of the application or Company Reputation* (connections 1, 2 and 3). Furthermore, these are also influenced by other, as depicted in connections 4, 5, and 6. Finally, *Media* takes a critical significance in the total model as it involves graphically the three factors and Perception of Trust itself.

For the sake of simplification, some factors encompassed the emerged categories. In the case of *Privacy Awareness*, it includes not only the idea that some of the participants have regarding the way that service providers (applications owners) protects the collected data, but also the participants' concerns regarding third-party surveillance, quantity and type of information shared. *Degree of Development of the application or Company Reputation* concerns participants' opinion on applications that are popular or that belong to big companies.

Exploitability of Information category refers to how the application providers use the information that users share by using an application, such as: for improving user-experience, the application itself, consuming trends, applying marketing strategies and for manipulating mass behaviors.

Media represents the information and influence caused by mass media, as the case of the internet news, newspaper and the ones that appear on television. Since none reported personal experience or friends opinions, direct social interaction tended to not have a strong influence in the model as itself.

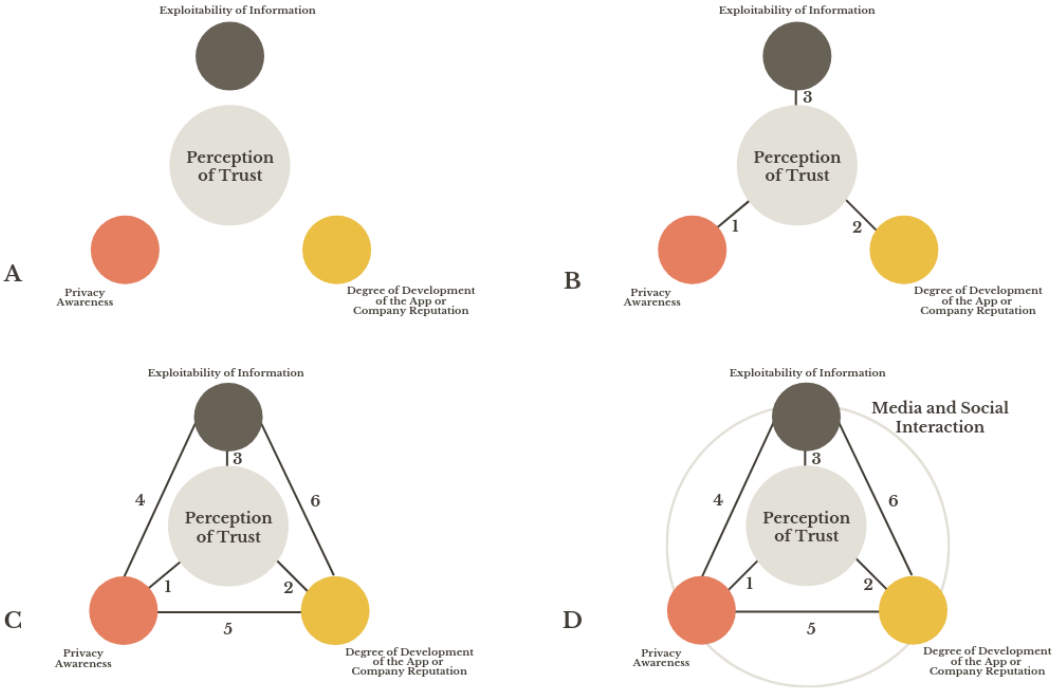


Figure 6.26: The chronology of the built model: A) where the main concepts emerged; B) where the direct connections with the perception of trust were firstly discovered; C) when trying to understand their interactions, the authors reached the conclusion of a direct influence among them; and finally D) where the role of the Media and Social interactions as included, influencing directly all factors.

6.3.3.1 Privacy Awareness

Participants' trust is directly related with *Privacy Awareness*, which can be justified by relating the superficially shared information (**connection 1**). Participants reported a lower trust with location-based applications, health and even social networks, where some level of direct information is prone to be extracted.

However, they did not feel this mistrust in applications that did not require a direct interaction or that the data sensing process is not noticeable. This, besides privacy, is also a problem of awareness; none of participant considered inference attacks from raw sensing data as accelerometer and gyroscope [Bai et al., 2017].

Participants may think their routine cannot be identified with applications that apart from a specific function like a game, are collecting sensor raw data. However, it does not necessarily mean that these are not sensing in background. This leads participants to think that a company that develops this kind of applications, for example, is not able to exploit information by other means (**connection 4**). Here is an example from two participants:

> "*... Social networks applications does not have much information about me. I barely post stuff on my mural. They can only see my*

> *conversations on the chat ... I delete all the built-in applications like maps and health applications but I do play games...(P2)*".

> "*...I believe that Maps (location-based app) saves only my locations, the places that I usually visit and perhaps my phone number...(P7)*".

6.3.3.2 Degree of development of the application

When an application is widely used or is provided by a renowned multinational, the perception of trust is altered (**connection 2**). When concerning two equally big companies, people tend to prefer the most used ones:

> "*...I don't use the the built-in applications from which I have similar ones in Google because they are better and easier to use"...(P1).*

> "*I prefer to use Google applications than Huawei's one, actually, I try to use all of them for my daily routine"...(P10).*

In fact, in most cases, this trust perception is influenced simultaneously by Privacy Awareness (**connection 5**) when one pays attention to the nature of information that an application needs to work properly: daily routine data or passwords, bank account credentials, among others. In terms of this data nature, perception of trust changes radically.

Participants that affirmed big companies would use every opportunity to make money by sharing data with third-parties for marketing studies, manipulating behaviour and other purposes, did not shared an equal mistrust regarding bank account information or passwords. In fact, when sharing these information, they preferred renowned companies or widely used applications, since participants consider these would have a strong security system to protect the data. Some examples:

> "*...I'm pretty sure big companies, if they can, they will sell everything. Their final goal is and it will always be money, profit... (P5)".*

> "*...Big Companies can sell the information to other parties for marketing reasons, to understand the market...(P10). ".*

> "*...In bank accounts and passwords, I believe applications like App-Store are very protected and secure...(P4)*".

> "*...I think that Apple saves all my keys and passwords in their private cloud that nobody else except me can access...(P9)*".

In terms of what people perceive regarding the use of people routine data. In a general way, people think big providers protect better their data from hackers or threats while the purpose of exploration of data is the reason of mistrust.

We could observe how participants trust small and big companies regarding handling more critical information as bank accounts credentials and passwords, where the big ones are preferred. In this case, people trust in both cases in

terms of information exploitation but they considered that the big company applications are more trustful in terms of security and information storage.

6.3.3.3 Exploitability of Information

People tend to trust more or less in an application depending how they perceive that the *Exploitation of Information* is done (**connection 3**). People that do not see marketing studies personalized for a user as bad, tend to trust more and use more freely applications. Moreover, others tend to claim that they allow to share more data to improve user experience only when they think the data will not be used for any other purpose.

> "*...I only let an application retrieve more information from me when I am sure that they are not going to use it for any other purpose than improving the application or user-experience...(P6)*".

> "*...I don't mind if they use my information for marketing reasons, as long as I have a good experience using the application is fine for me...(P8)* ".

> "*...I use the applications and it doesn't bother me that they use the information for marketing, since it is already done in commercials in TV and in real-life...(P3)* ".

If a company or application with a high level of development, that is, an application from a big company as the mentioned ones, people will assume the exploitation of information will be directed toward different uses that are not the one concerned with improving the application itself (**connection 6**). This leads people to trust less in the applications. However, when is a small company or a start-up, people directly assume the collected data will be used for improving the application.

> "*...Big Companies, if they get the chance to make money with the data, they will do it " ... If it is an application from a start-up company, I think they are only interested first in developing the application first...(P5)*".

6.3.3.4 Media and Social Interaction

Media is connected to all factors, since influences them: *Privacy Awareness*, *Degree of Development of the App or Company Reputation* and *Exploitability of Information*. The exploitation of information and the use of an application or the company reputation are directly related with the media, since many of the interviewers justified the majority of their opinions with news that they read or saw. When they did not explicitly justified the opinions with them, they mentioned facts that are from the public domain precisely because of the news. This trust is indirect, it is build on the recommendations and opinions, also know as transitive trust [Abdelghani et al., 2016].

These concerned the elections in the USA, security breaches and hacking attacks.

Furthermore, the idea one has if a company is more or less developed is also related with media news and social interaction.

> "*...Since I saw the news regarding USA elections, I don't trust as much in applications from Facebook or Twitter as I trust in Google ones...(P5)*".

> "*...I always have afraid of some hacker on Facebook or other social networks, as I have already read in some news...(P1)*".

6.3.4 Remarks

The final model was obtained through an iterative process of analyzing and coding the participants responses, as seen in Figure 6.26. When connections were made, it was attempted to understand the origin of the concepts that linked and its variability. In a first phase, some initial concepts appeared. In fact and as mentioned before, a higher number of concepts and smaller ones were obtained but for the sake of a simplified model, the concepts of *Exploitability of Information*, *Privacy Awareness* and *Degree of Development of an Application or Company Reputation* were the most prominent (phase A).

The next step was intuitive, achieving connections between every concept to the perception of trust model, as seen in phase B. However, when these links were performed, most of the participant answers that provided these conclusions had also a major influence from the other concepts. Due to this, it was concluded that the three concepts were also linked mutually, since they all influence each other (phase C).

The media and social interactions appeared later in phase D, where it was attempted to understand the origin of the participant opinions concerning providers, privacy and exploitation of information. Thus, and remembering the strong influence of the social factor in humans, media and social interactions were added as involving the whole scheme diagram, since all these concepts are immersed within common opinion and participant's beliefs. Specially the social interaction leads to the use of these applications, even when the perception of the trust that a user may have is not the best.

Nevertheless, some findings were relevant. For example, when we asked indirectly about privacy, all participants ended up moving their answers to trust without any intervention by the interviewer. In a generalized way, people seem to trust less in the use of information than in the protection of it.

Some justifications were related with the existence of protocols and legislation such as the GDPR, mentioned only by one of the participants (P11), and ironically from outside the EU. Besides the fact that a fault in information storage would be result in a tremendous damage to a company's reputation. This was also the motives why participants trusted in specific applications by renowned companies when sharing bank account details and passwords, since a major flaw in these systems would be unbearable to this kind of companies. Thus, even when participants trust in this kind of applications, it seems that is never for a

naive good reason but always for a profitable one.

Consequently, from the participants' opinion the providers should advertise to a certain extent their data handling, and safety strategies and how the information shared by users is processed, if they want to improve user's perception of trust. To big companies, it would be better to invest in advertising their use of information than in safety. Regarding small ones, it would be a better strategy to advertise their capability of preventing and defending themselves from cyber-attacks.

6.4 Summary

In this chapter, we have carried out quantitative validations and assessments of the proposed models implemented in this study, showcasing their effectiveness and feasibility. Additionally, we conducted a qualitative study focusing on a shared aspect among the case study implementations. The forthcoming chapter will provide a comprehensive overview of the work accomplished throughout the course of the PhD, along with the valuable contributions made to the field. Furthermore, we will engage in an insightful discussion, exploring potential future directions for further improvement and advancement.

Publications based on this chapter's work

- Rivadeneira, J. E., Jiménez, M. B., Marculescu, R., Rodrigues, A., Boavida, F., and Sá Silva, J. (2023b). A blockchain-based privacy-preserving model for consent and transparency in human-centered internet of things. In *Proceedings of the 8th ACM/IEEE Conference on Internet of Things Design and Implementation*, IoTDI '23, page 301–314, New York, NY, USA. Association for Computing Machinery;
- Rivadeneira, J. E., Borges, G. A., Rodrigues, A., Boavida, F., and Silva, J. S. (2023a). A unified privacy preserving model with ai at the edge for human-in-the-loop cyber-physical systems. *Submitted to Internet of Things; Engineering Cyber Physical Human Systems* **(Q1)**;
- Rivadeneira, J. E., Sánchez, O. T., Dias, M., Rodrigues, A., Boavida, F., and Silva, J. S. (2023d). Confluence: An integration model for human-in-the-loop iot privacy-preserving solutions towards sustainability in a smart city. *Submitted to IEEE Internet of Things Journal* **(Q1)**;
- Rivadeneira, J. E., Filipe Pinto, M., and Sá Silva, J. (2020). A qualitative study on trust perception in iot mobile applications. In *2020 IEEE Colombian Conference on Communications and Computing (COLCOM)*, pages 1–6;

Chapter 7

Conclusions and Future Work

Contents

The user-centric approach for privacy-preservation in HiTLCPSs proposed in this research shows promising potential for safeguarding user data, providing users with a way to control their data flows and promoting transparency. However, it is evident that there is still much ground to cover, especially concerning the seamless integration of emerging technologies. As we move forward, continued research and development efforts are necessary to address the challenges and complexities that arise in this rapidly evolving domain.

In this chapter, we summarize the developed work, highlight the contributions of this thesis, and look into the future challenges.

7.1 Synthesis of the Thesis

The work carried out in this thesis focused on providing solutions to address privacy preservation within the context of human-centric IoT-based systems, more specifically, HiTLCPS. The work was organized and presented as follows.

Chapter 2 offered an overview of the transformation of the conventional IoT concept into novel human-centric paradigms, where end-users and their data played a vital role while simultaneously highlighting privacy as a significant challenge within these frameworks. Subsequently, a thorough review and analysis of current user-centric privacy-preserving models followed, wherein they were categorized based on a proposed classification. This chapter was concluded by identifying and discussing challenges and open issues.

Next, in Chapter 3, we began by providing the concept, the process, and the importance of HiTLCPS in this new IoT era. We also highlighted that one of the most significant challenges in implementations based on this notion was privacy preservation. To address this concern, this chapter provided two privacy-preserving approaches, one oriented toward the data acquisition phase, and the other to the state-inference phase. For the first approach, this chapter described our privacy-aware framework called PACHA, its components, and the modules comprising them. The proposed privacy-preserving approach was built upon the features of this framework, emphasizing the consent management process and tackling the challenge related to transparency, by proposing the use of a permissioned blockchain to preserve the integrity of transactions derived from both data-sharing and consent actions. For the privacy-preserving approach, this chapter provided some background regarding AI at the edge and extended the current model with FL to carry out the state inference on the DO side. Finally, the chapter described a roadmap for the integration of multiple HiTLCPSs and the incorporation of Edge AI mechanisms at the DO domain for a future iteration of the current model.

In Chapter 4, we presented a model that integrated citizen-centric IoT privacy preservation solutions to foster the vision of smart and sustainable cities. This

chapter began by providing an overview of the background and related work in this area, identifying limitations, and providing the rationale for the current work. Later, we introduced our CONFLUENCE model, which was oriented to HiTLCPSs and aimed to define the necessary entities, components, and interactions for a privacy-preserving data sharing among the stakeholders that integrate a smart city. This model incorporated contemporary technologies like blockchain and LoRa. Moreover, this model included the description of a re-encryption scheme and incentives mechanism.

In Chapter 5, we introduced our two case studies, ISABELA and Green Bear, which exemplified the implementation of the HiTLCPS concept. Each of these case studies revolved around the deployment of distinct platforms, individually tailored to address different objectives in specific contexts. The presentation of the case studies included a description of FIWARE and its used in the implementation of ISABELA and Green Bear platforms. Subsequently, the chapter introduced SPACES, our unified platform with the objective of integrating the services offered by ISABELA and Green Bear while considering the components of the models proposed in Chapters 3 and 4. This chapter provided technical details regarding the development and implementation of these components and the selected underlying technology.

Chapter 6 addressed the assessments of the main components from the models proposed in Chapters 3 and 4 and their results. The first two sections of this chapter approached the evaluations from a quantitative perspective. Specifically, the first section addressed the privacy-preserving model, starting with its test environment description. Then, regarding the assessment, this section evaluated the IoT Broker response, the throughput and latency of the blockchain network, the impact of the re-encryption process, and also described the creation of an FL model and its validation using a dataset obtained in a trial of one of our previous case studies. The second section of this chapter addressed the integration model. Similar to the first one, this section described the prototype platform deployment, including the technical specifications. The round of assessments focused on the blockchain network implementation and the public IoT resources in a TTN network. Finally, this chapter concluded with a section dedicated to a qualitative study conducted to understand the perception of trust in IoT mobile applications, a relevant aspect shared by the platforms derived from the case studies described in the previous chapter, as well as the current platform. The description of this study included details regarding the participants, the type of approach, the qualitative method selection, the insights, and a discussion of the results.

7.2 Contributions

The research work conducted in the context of this thesis was driven by the objectives described in Chapter 1. With these objectives in mind, this thesis led to the contributions described below:

- **Review of the state-of-the-art regarding user-centric privacy pre-**

serving models In order to gain a comprehensive understanding of the current contributions in this field, and identify the gaps in the existing research we performed a literature review. We consider that this can be used by other researches as starting point to delve into the research field and fast track the development of novel proposals.

- **Creation of a classification for user-centric privacy-preserving models** In the state-of-the-art, proposals that revise and categorize user-centric privacy-preserving models in this particular IoT context are scarce. In order to establish a common language for the analysis, we have proposed a classification. Through this contribution, the aim is to provide a more structured guide that better directs new researchers in this field.
- **Creation of a new privacy-preserving model for HiTLCPSs** After studying the concept of HiTLCPS, we proposed two privacy-preserving approaches oriented toward the data acquisition and state inference phases, respectively. Based on these two approaches, a new privacy-preserving model for HiTLCPSs is created. This model can be used as a foundation for the development of new privacy-preserving HiTLCPSs.
- **Definition of a new framework for HiTLCPSs** From the reviewed models in the state of the art, we extracted certain features that were later used to build and define our framework. This framework, named PACHA, was then utilized in the development of our initial approach, which includes the privacy-preserving model. PACHA defines a comprehensive privacy-preserving data sharing architecture among stakeholders. The functionalities defined in this framework have been incorporated into the components of the models proposed in this thesis.
- **Creation of a new decentralized consent management procedure for HiTLCPSs** One component that integrates the data acquisition phase of our privacy-preserving model is consent management. In this regard, one of our contributions is the development of a decentralized consent management process to enhance transparency. This procedure consists of five phases and involves all the entities of the model with their respective components.
- **Development of a new HiTLCPS case study** Alongside the implementation of the privacy model, we also developed a new case study proposal focused on the sustainability of smart cities. This case study, known as Green Bear, aims to enable citizens to assess their involvement in aspects that enhance the city's sustainability through a gamification scheme. Participants can earn points for engaging in various activities in the city's public spaces and taking personal actions to improve their quality of life.
- **Creation of a new model for integrating privacy-preserving HiTLCPSs** After proposing the privacy preservation model, the subsequent step involved creating a solution that enables the integration of various privacy-preserving HiTLCPSs to address a specific requirement. In our case, our model is oriented toward promoting sustainability in smart

cities, leveraging our aforementioned case study. However, we believe that to make a significant change in the city's sustainability, it is necessary to integrate multiple services proposed by HiTLCPSs from different contexts that consider privacy aspects from their design.

- **Creation of a new platform that integrates different services from stand-alone HiTLCPSs** As it is observed that the systems used in ISABELA and Green Bear share common characteristics but are managed individually, resulting in duplicated efforts, the creation of an integral platform has been proposed. This platform will allow the implementation and comprehensive channeling of services offered by these individual systems.
- **Development of a FL model for state inference in HiTLCPSs** In our HiTLCPS case studies, the inference process has traditionally been conducted using machine learning models on servers outside the user's control (e.g., servers in a cloud managed by the responsible inference process). To establish an inference process that does not require data to leave the user's device, we employed FL and developed a new model. Although our FL-based proposal delivered a slightly lower level of accuracy compared to the traditional machine learning model, the former ensures privacy preservation during the state inference phase.

In addition to the contributions described above the work conducted in this thesis directly led to publications in international journals and international conferences. We would like to highlight specially the publications on journals of the first quartile. Additionally, it also led to active cooperation inside and outside the research group which, in turn, contributed to several joint publications.

7.3 Future Work

During our review of the state of the art within the context of this thesis, we have found that efforts to develop systems aligned with principles such as 'Privacy by Design' date back to the times of 'Ubiquitous Computing'. However, since the proposal and enforcement of regulations aimed at the protection of personal data worldwide, we have observed a significant increase in contributions. This growth reflects a genuine concern for preserving privacy, which, in turn, presents an ongoing challenge, especially in the new human-centric concepts, a result of the evolution of the 'Internet of Things' paradigm.

Data protection and control have never been as important as nowadays. Although our thesis revolves around and contributes to this topic by proposing a user-centric, privacy-preserving model, we believe that there is still plenty of room for further work. For instance, regarding the first proposed approach that comprises our model, a challenge can arise if the threat model is extended by considering a scenario where malicious IoT Brokers and DRs collude to gain access to more data from IoT resources than approved by the DO. To overcome this limitation and control the re-encryption capacity of the IoT Brokers, a future model iteration could explore, incorporate, and validate an enhanced encryption

approach (e.g., conditional and accountable proxy re-encryption).

Regarding the overall consent procedures, the current consent request process does not foresee the possibility for a DR to select IoT resources based on their locations, as this would disclose the position of the user in the case of mobile IoT resources. Another aspect to consider is the possibility for DRs to waive the granted consent if the data do not satisfy their needs. Furthermore, the data deletion request process could be enriched by coupling an InterPlanetary File System, where access to the stored data is removed after a consent revocation. These considerations could be taken into account for an enhanced version of this model in a future proposal.

In the case of the second approach of the model, the feasibility of the proposed roadmap still needs validation, particularly concerning the state inference process at the IoT resource level. Additionally, new mechanisms based on reinforcement learning techniques might be studied and taken into account for future work. We consider that exploring and integrating these techniques would allow greater interaction with DOs to refine their learning models as the basis of HiTL services, whether at the level of IoT Gateways or IoT Resources, and also address ethical issues within services from different contexts.

Regarding the implementation of the models, we believe that future work could involve deploying them with a larger number of interacting devices. This would allow for invaluable insights into the scalability of our proposals and identify areas for further improvement. In addition to quantitative measures, we also recognize the significance of qualitative evaluation. Specifically, in the case of our integral model, the system should be carefully assessed through the lens of the three pillars of sustainability, encompassing environmental, social, and economic dimensions. Qualitative evaluation could provide a deeper understanding of user experiences, perceptions, interactions and attitudes toward privacy, complementing the technical assessments. This comprehensive approach would help us assess the system's impact and effectiveness in promoting sustainable practices within a real deployment environment. Moreover, in the context of future work, it is crucial to validate the proposed incentive mechanism as outlined in the thesis. The successful validation of this mechanism holds the potential to address one of the most vexing challenges encountered in the implementation of HiTLCPSs, namely, the issue of user participation.

To sum up, by implementing a user-centric privacy-preserving model, individuals can maintain control over their sensitive data, aligning with the principles of data protection mandated by most regulations. Moreover, the use of Edge AI and FL techniques further enhances privacy by minimizing the transmission and centralization of personal information, thus reducing the risks of data breaches and unauthorized access. However, it is crucial to acknowledge the challenges and counter-effects that may arise by interoperating across different IoT domains, especially in the case of Healthcare where specific requirements from regulations, like Health Insurance Portability and Accountability Act (HIPAA), must be considered, such as consent and data de-identification, to ensure compliance with healthcare data privacy standards. Similarly, aligning with GDPR

principles, such as lawful data processing, individual rights, and cross-border data transfers, addresses the regulations' comprehensive approach to data protection. Risk analysis tasks and continuous monitoring of the proposed systems are necessary to identify and mitigate potential vulnerabilities and ensure ongoing compliance with regulations.

Bibliography

Abdelghani, W., Zayani, C. A., Amous, I., and Sèdes, F. (2016). Trust management in social internet of things: A survey. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 9844 LNCS, pages 430–441. Springer Verlag.

Agarwal, R. R., Kumar, D., Golab, L., and Keshav, S. (2020). Consentio: Managing consent to data access using permissioned blockchains. In *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–9.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4):2347–2376.

Alhajri, M., Rudolph, C., and Shahraki, A. S. (2022a). A blockchain-based consent mechanism for access to fitness data in the healthcare context. *IEEE Access*, 10:22960–22979.

Alhajri, M., Salehi Shahraki, A., and Rudolph, C. (2022b). Privacy of fitness applications and consent management in blockchain. In *Proceedings of the 2022 Australasian Computer Science Week*, ACSW '22, page 65–73, New York, NY, USA. Association for Computing Machinery.

Almalki, F. A., Alsamhi, S. H., Sahal, R., Hassan, J., Hawbani, A., Rajput, N. S., Saif, A., Morgan, J., and Breslin, J. (2021). Green iot for eco-friendly and sustainable smart cities: Future directions and opportunities. *Mobile Networks and Applications*.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Cocco, S. W., and Yellick, J. (2018). Hyperledger fabric: A distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference*, EuroSys '18, New York, NY, USA. Association for Computing Machinery.

Armando, N., Rodrigues, A., Pereira, V., Sá Silva, J., and Boavida, F. (2018). An outlook on physical and virtual sensors for a socially interactive internet. *Sensors*, 18(8).

Arnaudo, M., Gerrits, L., Grishkov, I., Kromes, R., and Verdier, F. (2023). Blockchains accesses for low-power embedded devices using lorawan. In *Proceedings of the 12th International Conference on the Internet of Things*, IoT '22, page 119–126, New York, NY, USA. Association for Computing Machinery.

Attia, T., Heusse, M., Tourancheau, B., and Duda, A. (2019). Experimental characterization of lorawan link quality. In *2019 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6.

Atzori, L., Iera, A., Morabito, G., and Nitti, M. (2012). The social internet of things (siot) - when social networks meet the internet of things: Concept, architecture and network characterization. *Computer Networks*, 56(16):3594–3608.

Bai, X., Yin, J., and Wang, Y. P. (2017). Sensor guardian: prevent privacy inference on android sensors. *Eurasip Journal on Information Security*, 2017.

Banerjee, S., Odelu, V., Das, A. K., Srinivas, J., Kumar, N., Chattopadhyay, S., and Choo, K.-K. R. (2019). A provably secure and lightweight anonymous user authenticated session key exchange scheme for internet of things deployment. *IEEE Internet of Things Journal*, 6(5):8739–8752.

Barhamgi, M., Perera, C., Ghedira, C., and Benslimane, D. (2018). User-centric privacy engineering for the internet of things. *IEEE Cloud Computing*, 5(5):47–57.

Barnett, T., Jain, S., Andra, U., and Khurana, T. (2018). Cisco visual networking index (vni) complete forecast update, 2017–2022. *Americas/EMEAR Cisco Knowledge Network (CKN) Presentation*, pages 1–30.

Bermejo Fernandez, C., Lee, L. H., Nurmi, P., and Hui, P. (2021). Para: Privacy management and control in emerging iot ecosystems using augmented reality. In *Proceedings of the 2021 International Conference on Multimodal Interaction*, ICMI '21, page 478–486, New York, NY, USA. Association for Computing Machinery.

Bhardwaj, K., Chen, W., and Marculescu, R. (2020). Invited: New directions in distributed deep learning: Bringing the network at forefront of iot design. In *2020 57th ACM/IEEE Design Automation Conference (DAC)*, pages 1–6.

Bhardwaj, K., Lin, C.-Y., Sartor, A., and Marculescu, R. (2019a). Memory- and communication-aware model compression for distributed deep learning inference on iot. *ACM Trans. Embed. Comput. Syst.*, 18(5s).

Bhardwaj, K., Suda, N., and Marculescu, R. (2019b). Dream distillation: A data-independent model compression framework. *arXiv*.

Bhardwaj, K., Suda, N., and Marculescu, R. (2021). Edgeal: A vision for deep learning in the iot era. *IEEE Design & Test*, 38(4):37–43.

Boavida, F., Kliem, A., Renner, T., Riekki, J., Jouvray, C., Jacovi, M., Ivanov, S., Guadagni, F., Gil, P., and Triviño, A. (2016). People-centric internet of things—challenges, approach, and enabling technologies. In Novais, P., Camacho, D., Analide, C., El Fallah Seghrouchni, A., and Badica, C., editors, *Intelligent Distributed Computing IX*, pages 463–474, Cham. Springer International Publishing.

Bobolz, J., Eidens, F., Krenn, S., Slamanig, D., and Striecks, C. (2020). Privacy-preserving incentive systems with highly efficient point-collection. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, ASIA CCS '20, page 319–333, New York, NY, USA. Association for Computing Machinery.

Bonawitz, K., Eichner, H., Grieskamp, W., Huba, D., Ingerman, A., Ivanov, V., Kiddon, C., Konečný, J., Mazzocchi, S., McMahan, H. B., Overveldt, T. V., Petrou, D., Ramage, D., and Roselander, J. (2019). Towards federated learning at scale: System design. *arXiv*.

Boubiche, D. E., Imran, M., Maqsood, A., and Shoaib, M. (2019). Mobile crowd sensing – taxonomy, applications, challenges, and solutions. *Computers in Human Behavior*, 101:352–370.

Brutti, A., De Sabbata, P., Frascella, A., Gessa, N., Ianniello, R., Novelli, C., Pizzuti, S., and Ponti, G. (2019). *Smart City Platform Specification: A Modular Approach to Achieve Interoperability in Smart Cities*, pages 25–50. Springer International Publishing, Cham.

Cate, F. H. (2006). The failure of fair information practice principles. *Consumer protection in the age of the information economy*.

Cha, S.-C., Chuang, M.-S., Yeh, K.-H., Huang, Z.-J., and Su, C. (2018). A user-friendly privacy framework for users to achieve consents with nearby ble devices. *IEEE Access*, 6:20779–20787.

Chakraborty, S., Shen, C., Raghavan, K. R., Shoukry, Y., Millar, M., and Srivastava, M. (2014). Ipshield: A framework for enforcing context-aware privacy. In *Proceedings of the 11th USENIX Conference on Networked Systems Design and Implementation*, NSDI'14, page 143–156, USA. USENIX Association.

Chander, A. and Land, M. (2014). Introductory note to united nations general assembly resolution on the right to privacy in the digital age. *International Legal Materials*, 53(4):727–731.

Chaudhry, A., Crowcroft, J., Howard, H., Madhavapeddy, A., Mortier, R., Haddadi, H., and McAuley, D. (2015). Personal data: Thinking inside the box. In *Proceedings of The Fifth Decennial Aarhus Conference on Critical Alternatives*, CA '15, page 29–32, Aarhus N. Aarhus University Press.

Chen, Y., Qin, X., Wang, J., Yu, C., and Gao, W. (2020). Fedhealth: A federated transfer learning framework for wearable healthcare. *IEEE Intelligent Systems*, 35(4):83–93.

Chhetri, C. and Genaro Motti, V. (2022a). Designing and evaluating a prototype for data-related privacy controls in a smart home. In *Human Aspects of Information Security and Assurance*, pages 240–250, Cham. Springer International Publishing.

Chhetri, C. and Genaro Motti, V. (2022b). User-centric privacy controls for smart homes. *Proc. ACM Hum.-Comput. Interact.*, 6(CSCW2).

Chi, P.-Y. P., Batra, A., and Hsu, M. (2018). Mobile crowdsourcing in the wild: Challenges from a global community. In *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct*, MobileHCI '18, page 410–415, New York, NY, USA. Association for Computing Machinery.

Chow, R. (2017). The last mile for iot privacy. *IEEE Security & Privacy*, 15(6):73–76.

Colnago, J., Feng, Y., Palanivel, T., Pearman, S., Ung, M., Acquisti, A., Cranor, L. F., and Sadeh, N. (2020). Informing the design of a personalized privacy assistant for the internet of things. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–13, New York, NY, USA. Association for Computing Machinery.

Commission, E. (2016). Article29 newsroom - guidelines on consent under regulation 2016/679 (wp259rev.01) - european commission.

Commission, E., Directorate-General for Communications Networks, C., Technology, and for Informatics, D.-G. (2021). *Proposal for a European Interoperability Framework for Smart Cities and Communities (EIF4SCC)*. Publications Office of the European Union.

Contissa, G., Docter, K., Lagioia, F., Lippi, M., Micklitz, H.-W., Pałka, P., Sartor, G., and Torroni, P. (2018). Claudette meets gdpr: Automating the evaluation of privacy policies using artificial intelligence. *SSRN*.

Corcoran, P. M. (2016). A privacy framework for the internet of things. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pages 13–18.

Cranor, L. (2003). P3p: making privacy policies more useful. *IEEE Security & Privacy*, 1(6):50–55.

Cranor, L., Langheinrich, M., and Marchiori, M. (2002). A p3p preference exchange language 1.0 (appel1. 0). *http://www. w3c. org/TR/P3P-preferences. html*.

Dahouda, M. K. and Joe, I. (2021). A deep-learned embedding technique for categorical features encoding. *IEEE Access*, 9:114381–114391.

Dai, W., Qiu, M., Qiu, L., Chen, L., and Wu, A. (2017). Who moved my data? privacy protection in smartphones. *IEEE Communications Magazine*, 55(1):20–25.

Das, A., Degeling, M., Smullen, D., and Sadeh, N. (2018). Personalized privacy assistants for the internet of things: Providing users with notice and choice. *IEEE Pervasive Computing*, 17(3):35–46.

Das, A., Degeling, M., Wang, X., Wang, J., Sadeh, N., and Satyanarayanan, M. (2017). Assisting users in a world full of cameras: A privacy-aware infrastructure for computer vision applications. In *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pages 1387–1396.

Datta, T., Apthorpe, N., and Feamster, N. (2018). A developer-friendly library for smart home iot privacy-preserving traffic obfuscation. In *Proceedings of the 2018 Workshop on IoT Security and Privacy*, page 43–48, New York, NY, USA. Association for Computing Machinery.

Davies, N., Taft, N., Satyanarayanan, M., Clinch, S., and Amos, B. (2016). Privacy mediators: Helping iot cross the chasm. In *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications*, HotMobile '16, page 39–44, New York, NY, USA. Association for Computing Machinery.

Diamantopoulou, V., Angelopoulos, K., Flake, J., Praitano, A., Ruiz, J. F., Jürjens, J., Pavlidis, M., Bonutto, D., Sanz, A. C., Mouratidis, H., Robles, J. G., and Tozzi, A. E. (2017). Privacy data management and awareness for public administrations: A case study from the healthcare domain. In Schweighofer, E., Leitold, H., Mitrakas, A., and Rannenberg, K., editors, *Privacy Technologies and Policy*, pages 192–209, Cham. Springer International Publishing.

Eckhoff, D. and Wagner, I. (2018). Privacy in the smart city—applications, technologies, challenges, and solutions. *IEEE Communications Surveys & Tutorials*, 20(1):489–516.

Edwards, L. (2016). Privacy, security and data protection in smart cities: A critical eu law perspective. *SSRN Electronic Journal*.

Egala, B. S., Pradhan, A. K., Badarla, V., and Mohanty, S. P. (2021). Fortified-chain: A blockchain-based framework for security and privacy-assured internet of medical things with effective access control. *IEEE Internet of Things Journal*, 8(14):11717–11731.

Fernandes, J., Raposo, D., Armando, N., Sinche, S., Silva, J. S., Rodrigues, A., Pereira, V., Oliveira, H. G., Macedo, L., and Boavida, F. (2020). Isabela – a socially-aware human-in-the-loop advisor system. *Online Social Networks and Media*, 16:100060.

Fernandes, J., Raposo, D., Sinche, S., Armando, N., Silva, J. S., Rodrigues, A., Macedo, L., Oliveira, H. G., and Boavida, F. (2019). A human-in-the-loop cyber-physical approach for students performance assessment. In *Proceedings of the Fourth International Workshop on Social Sensing*, SocialSense'19, page 36–42, New York, NY, USA. Association for Computing Machinery.

Firoozjaei, M. D., Lu, R., and Ghorbani, A. A. (2020). An evaluation framework for privacy-preserving solutions applicable for blockchain-based internet-of-things platforms. *Security and Privacy*, 3(6):e131.

Frakes, W. and Kang, K. (2005). Software reuse research: status and future. *IEEE Transactions on Software Engineering*, 31(7):529–536.

Gong, W., Zhang, B., and Li, C. (2019). Privacy-aware online task assignment framework for mobile crowdsensing. In *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, pages 1–6.

Gopstein, A., Nguyen, C., O'Fallon, C., Hastings, N., and Wollman, D. A. (2021). Nist framework and roadmap for smart grid interoperability standards, release 4.0.

Grace, P. and Surridge, M. (2017). Towards a model of user-centered privacy preservation. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*, ARES '17, pages 1–8, New York, NY, USA. Association for Computing Machinery.

Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M. (2013). Internet of things (iot): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7):1645–1660. Including Special sections: Cyber-enabled Distributed Computing for Ubiquitous Cloud and Network Services & Cloud Computing and Scientific Applications — Big Data, Scalable Analytics, and Beyond.

Guillén, J., Miranda, J., Berrocal, J., García-Alonso, J., Murillo, J. M., and Canal, C. (2014). People as a service: A mobile-centric model for providing collective sociological profiles. *IEEE Software*, 31(2):48–53.

Guo, B., Zhang, D., Wang, Z., Yu, Z., and Zhou, X. (2013). Opportunistic iot: Exploring the harmonious interaction between human and the internet of things. *Journal of Network and Computer Applications*, 36(6):1531–1539.

Guo, H., Zhang, Z., Xu, J., An, N., and Lan, X. (2021). Accountable proxy re-encryption for secure data sharing. *IEEE Transactions on Dependable and Secure Computing*, 18(1):145–159.

Halcu, I., Nunes, D., Sgârciu, V., and Silva, J. S. (2015). New mechanisms for privacy in human-in-the-loop cyber-physical systems. In *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, volume 1, pages 418–423.

Han, S., Mao, H., and Dally, W. J. (2015). Deep compression: Compressing deep neural networks with pruning, trained quantization and huffman coding. *arXiv*.

Hinton, G., Vinyals, O., and Dean, J. (2015). Distilling the knowledge in a neural network. *arXiv*.

Hochreiter, S. and Schmidhuber, J. (1997). Long short-term memory. *Neural Comput.*, 9(8):1735–1780.

Hoepman, J.-H. (2014). Privacy design strategies. In Cuppens-Boulahia, N., Cuppens, F., Jajodia, S., Abou El Kalam, A., and Sans, T., editors, *ICT Systems Security and Privacy Protection*, pages 446–459, Berlin, Heidelberg. Springer Berlin Heidelberg.

Honar Pajooh, H., Rashid, M., Alam, F., and Demidenko, S. (2021). Hyperledger fabric blockchain for securing the edge internet of things. *Sensors*, 21(2).

Jaimunk, J. (2019). Privacy-preserving cloud-iot architecture. In *Proceedings of the 6th International Conference on Mobile Software Engineering and Systems*, MOBILESoft '19, page 146–147. IEEE Press.

Jiménez, M. B., Fernández, D., Rivadeneira, J. E., Bellido, L., and Cárdenas, A. (2021). A survey of the main security issues and solutions for the sdn architecture. *IEEE Access*, 9:122016–122038.

Jin, H., Su, L., Xiao, H., and Nahrstedt, K. (2018). Incentive mechanism for privacy-aware data aggregation in mobile crowd sensing systems. *IEEE/ACM Transactions on Networking*, 26(5):2019–2032.

Kagal, L., Finin, T., and Joshi, A. (2003). A policy language for a pervasive computing environment. In *Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks*, pages 63–74.

Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Nitin Bhagoji, A., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R., D'Oliveira, R. G. L., Eichner, H., El Rouayheb, S., Evans, D., Gardner, J., Garrett, Z., Gascón, A., Ghazi, B., Gibbons, P. B., Gruteser, M., Harchaoui, Z., He, C., He, L., Huo, Z., Hutchinson, B., Hsu, J., Jaggi, M., Javidi, T., Joshi, G., Khodak, M., Konecný, J., Korolova, A., Koushanfar, F., Koyejo, S., Lepoint, T., Liu, Y., Mittal, P., Mohri, M., Nock, R., Özgür, A., Pagh, R., Qi, H., Ramage, D., Raskar, R., Raykova, M., Song, D., Song, W., Stich, S. U., Sun, Z., Suresh, A. T., Tramèr, F., Vepakomma, P., Wang, J., Xiong, L., Xu, Z., Yang, Q., Yu, F. X., Yu, H., and Zhao, S. (2021). Advances and open problems in federated learning. *Found. Trends Mach. Learn.*, 14(1–2):1–210.

Kanwal, T., Anjum, A., and Khan, A. (2021). Privacy preservation in e-health cloud: Taxonomy, privacy requirements, feasibility analysis, and opportunities. *Cluster Computing*, 24(1):293–317.

Kazemi, L. and Shahabi, C. (2011). Towards preserving privacy in participatory sensing. In *2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, pages 328–331.

Kazemi, L. and Shahabi, C. (2013). Tapas: Trustworthy privacy-aware participatory sensing. *Knowl. Inf. Syst.*, 37(1):105–128.

Keshavarz, M. and Anwar, M. (2018). Towards improving privacy control for smart homes: A privacy decision framework. In *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, pages 1–3.

Khan, L. U., Saad, W., Han, Z., Hossain, E., and Hong, C. S. (2021). Federated learning for internet of things: Recent advances, taxonomy, and open challenges. *IEEE Communications Surveys & Tutorials*, 23(3):1759–1799.

Khang, A., Chowdhury, S., and Sharma, S. (2022a). *The Data-Driven Blockchain Ecosystem: Fundamentals, Applications, and Emerging Technologies*. CRC Press.

Khang, A., Rani, S., and Sivaraman, A. K. (2022b). *AI-Centric Smart City Ecosystems: Technologies, Design and Implementation*. CRC Press.

Koh, J. Y., Peters, G. W., Leong, D., Nevat, I., and Wong, W.-C. (2017). Privacy-aware incentive mechanism for mobile crowd sensing. In *2017 IEEE International Conference on Communications (ICC)*, pages 1–6.

Koohang, A., Sargent, C. S., Nord, J. H., and Paliszkiewicz, J. (2022). Internet of things (iot): From awareness to continued use. *International Journal of Information Management*, 62:102442.

Kounoudes, A. D. and Kapitsaki, G. M. (2020). A mapping of iot user-centric privacy preserving approaches to the gdpr. *Internet of Things*, 11:100179.

Kounoudes, A. D., Kapitsaki, G. M., Katakis, I., and Milis, M. (2021). User-centred privacy inference detection for smart home devices. In *2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI)*, pages 210–218.

Kröger, J. (2019). Unexpected inferences from sensor data: A hidden privacy threat in the internet of things. In *Internet of Things. Information Processing in an Increasingly Connected World*, pages 147–159, Cham. Springer International Publishing.

Kröger, J. L., Raschke, P., and Bhuiyan, T. R. (2019). Privacy implications of accelerometer data: A review of possible inferences. In *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, ICCSP '19, page 81–87, New York, NY, USA. Association for Computing Machinery.

Kulkarni, P., Kirkham, R., and McNaney, R. (2022). Opportunities for smartphone sensing in e-health research: A narrative review. *Sensors*, 22(10).

Kumar, N., Aujla, G. S., Das, A. K., and Conti, M. (2019). Eccauth: A secure authentication protocol for demand response management in a smart grid system. *IEEE Transactions on Industrial Informatics*, 15(12):6572–6582.

Kumar, P., Kumar, R., Srivastava, G., Gupta, G. P., Tripathi, R., Gadekallu, T. R., and Xiong, N. N. (2021). Ppsf: A privacy-preserving and secure framework using blockchain-based machine-learning for iot-driven smart cities. *IEEE Transactions on Network Science and Engineering*, 8(3):2326–2341.

Kundu, D. (2019). Blockchain and trust in a smart city. *Environment and Urbanization ASIA*, 10(1):31–43.

Kusumastuti, R. D., Nurmala, N., Rouli, J., and Herdiansyah, H. (2022). Analyzing the factors that influence the seeking and sharing of information on the smart city digital platform: Empirical evidence from indonesia. *Technology in Society*, 68:101876.

Lafontaine, E., Sabir, A., and Das, A. (2021). Understanding people's attitude and concerns towards adopting iot devices. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI EA '21, pages 1–10, New York, NY, USA. Association for Computing Machinery.

Lane, N. D., Eisenman, S. B., Musolesi, M., Miluzzo, E., and Campbell, A. T. (2008). Urban sensing systems: Opportunistic or participatory? In *Proceedings of the 9th Workshop on Mobile Computing Systems and Applications*, HotMobile '08, page 11–16, New York, NY, USA. Association for Computing Machinery.

Langheinrich, M. (2001). Privacy by design — principles of privacy-aware ubiquitous systems. In Abowd, G. D., Brumitt, B., and Shafer, S., editors, *Ubicomp 2001: Ubiquitous Computing*, pages 273–291, Berlin, Heidelberg. Springer Berlin Heidelberg.

Langheinrich, M. (2002). A privacy awareness system for ubiquitous computing environments. In Borriello, G. and Holmquist, L. E., editors, *UbiComp 2002: Ubiquitous Computing*, pages 237–245, Berlin, Heidelberg. Springer Berlin Heidelberg.

Langley, D. J., van Doorn, J., Ng, I. C., Stieglitz, S., Lazovik, A., and Boonstra, A. (2021). The internet of everything: Smart things and their impact on business models. *Journal of Business Research*, 122:853–863.

Lashkari, B., Rezazadeh, J., Farahbakhsh, R., and Sandrasegaran, K. (2019). Crowdsourcing and sensing for indoor localization in iot: A review. *IEEE Sensors Journal*, 19(7):2408–2434.

Lee, G. Y., Cha, K. J., and Kim, H. J. (2019). Designing the gdpr compliant consent procedure for personal information collection in the iot environment. In *2019 IEEE International Congress on Internet of Things (ICIOT)*, pages 79–81.

Lee, H., Chow, R., Haghighat, M. R., Patterson, H. M., and Kobsa, A. (2018). Iot service store: A web-based system for privacy-aware iot service discovery and interaction. In *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 107–112.

Lejeune, C. (2019). *Manuel d'analyse qualitative*. De Boeck Supérieur.

Li, D., Wong, W. E., and Guo, J. (2020). A survey on blockchain for enterprise using hyperledger fabric and composer. In *2019 6th International Conference on Dependable Systems and Their Applications (DSA)*, pages 71–80.

Lin, C., He, D., Zeadally, S., Huang, X., and Liu, Z. (2021). Blockchain-based data sharing system for sensing-as-a-service in smart cities. *ACM Transactions on Internet Technology (TOIT)*, 21(2):1–21.

Lin, G., Wang, H., Wan, J., Zhang, L., and Huang, J. (2022). A blockchain-based fine-grained data sharing scheme for e-healthcare system. *Journal of Systems Architecture*, 132:102731.

Lippi, M., Contissa, G., Lagioia, F., Micklitz, H.-W., Pałka, P., Sartor, G., and Torroni, P. (2019). Consumer protection requires artificial intelligence. *Nature Machine Intelligence*, 1(4):168–169.

Liu, B., Andersen, M. S., Schaub, F., Almuhimedi, H., Zhang, S. A., Sadeh, N., Agarwal, Y., and Acquisti, A. (2016). Follow my recommendations: A personalized privacy assistant for mobile app permissions. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 27–41, Denver, CO. USENIX Association.

Liu, C., Zeng, Q., Cheng, L., Duan, H., Zhou, M., and Cheng, J. (2021). Privacy-preserving behavioral correctness verification of cross-organizational workflow with task synchronization patterns. *IEEE Transactions on Automation Science and Engineering*, 18(3):1037–1048.

Liu, J., Zhang, C., and Fang, Y. (2018). Epic: A differential privacy framework to defend smart homes against internet traffic analysis. *IEEE Internet of Things Journal*, 5(2):1206–1217.

Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., and Ni, W. (2020). Privysharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Computers & Security*, 88:101653.

Manzoor, A., Braeken, A., Kanhere, S. S., Ylianttila, M., and Liyanage, M. (2021). Proxy re-encryption enabled secure and anonymous iot data sharing platform based on blockchain. *Journal of Network and Computer Applications*, 176:102917.

Markovic, M., Asif, W., Corsar, D., Jacobs, N., Edwards, P., Rajarajan, M., and Cottrill, C. (2018). Towards automated privacy risk assessments in iot systems. In *Proceedings of the 5th Workshop on Middleware and Applications for the Internet of Things*, M4IoT'18, page 15–18, New York, NY, USA. Association for Computing Machinery.

Martínez, J. A., Hernández-Ramos, J. L., Beltrán, V., Skarmeta, A., and Ruiz, P. M. (2017). A user-centric internet of things platform to empower users for managing security and privacy concerns in the internet of energy. *International Journal of Distributed Sensor Networks*, 13(8).

McMahan, B., Moore, E., Ramage, D., Hampson, S., and Arcas, B. A. y. (2017). Communication-efficient learning of deep networks from decentralized data. In Singh, A. and Zhu, J., editors, *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, volume 54 of *Proceedings of Machine Learning Research*, pages 1273–1282. PMLR.

Mehrotra, S., Kobsa, A., Venkatasubramanian, N., and Rajagopalan, S. R. (2016). Tippers: A privacy cognizant iot environment. In *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, pages 1–6.

Miller, D. C. and Salkind, N. J. (2002). *Handbook of research design and social measurement*. Sage.

Miranda, J., Mäkitalo, N., Garcia-Alonso, J., Berrocal, J., Mikkonen, T., Canal, C., and Murillo, J. M. (2015). From the internet of things to the internet of people. *IEEE Internet Computing*, 19(2):40–47.

Miraz, M. H., Ali, M., Excell, P. S., and Picking, R. (2015). A review on internet of things (iot), internet of everything (ioe) and internet of nano things (iont). In *2015 Internet Technologies and Applications (ITA)*, pages 219–224.

Morel, V., Cunche, M., and Le Métayer, D. (2019). A generic information and consent framework for the iot. In *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pages 366–373.

Muhander, B. A., Rana, O., Arachchilage, N., and Perera, C. (2022). Demo abstract: Privacycube: A tangible device for improving privacy awareness in iot. In *2022 IEEE/ACM Seventh International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pages 109–110.

Munjin, D. and Morin, J.-H. (2011). User empowerment in the internet of things.

Nature (2021). Collaborative learning without sharing data. *Nature Machine Intelligence*, 3(6):459–459.

Nepal, S., Ko, R. K. L., Grobler, M., and Camp, L. J. (2022). Editorial: Human-centric security and privacy. *Frontiers in Big Data*, 5.

Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., and Vincent Poor, H. (2021). Federated learning for internet of things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 23(3):1622–1658.

Notario, N., Crespo, A., Kung, A., Kroener, I., Le Métayer, D., Troncoso, C., del Álamo, J. M., and Martín, Y. S. (2014). Pripare: A new vision on engineering privacy and security by design. In Cleary, F. and Felici, M., editors, *Cyber Security and Privacy*, pages 65–76, Cham. Springer International Publishing.

Nunes, D. S., Zhang, P., and Sá Silva, J. (2015). A survey on human-in-the-loop applications towards an internet of all. *IEEE Communications Surveys & Tutorials*, 17(2):944–965.

Nyst, C. and Falchetta, T. (2017). The Right to Privacy in the Digital Age. *Journal of Human Rights Practice*, 9(1):104–118.

Obour Agyekum, K. O.-B., Xia, Q., Sifah, E. B., Gao, J., Xia, H., Du, X., and Guizani, M. (2019). A secured proxy-based data sharing module in iot environments using blockchain. *Sensors*, 19(5).

Pal, S. and Mitra, S. (1992). Multilayer perceptron, fuzzy sets, and classification. *IEEE Transactions on Neural Networks*, 3(5):683–697.

Pappachan, P., Degeling, M., Yus, R., Das, A., Bhagavatula, S., Melicher, W., Naeini, P. E., Zhang, S., Bauer, L., Kobsa, A., Mehrotra, S., Sadeh, N., and Venkatasubramanian, N. (2017). Towards privacy-aware smart buildings: Capturing, communicating, and enforcing privacy policies and preferences. In *2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, pages 193–198.

Pardo, R. and Le Métayer, D. (2019). Analysis of privacy policies to enhance informed consent. In Foley, S. N., editor, *Data and Applications Security and Privacy XXXIII*, pages 177–198, Cham. Springer International Publishing.

Parliament, E. et al. (2016). Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation).

Party, A. . D. P. W. (2018). Guidelines on transparency under regulation 2016/679 (wp260rev.01) - european commission.

Perera, C., McCormick, C., Bandara, A. K., Price, B. A., and Nuseibeh, B. (2016). Privacy-by-design framework for assessing internet of things applications and platforms. In *Proceedings of the 6th International Conference on the Internet of Things*, IoT'16, page 83–92, New York, NY, USA. Association for Computing Machinery.

Petrov, V., Mikhaylov, K., Moltchanov, D., Andreev, S., Fodor, G., Torsner, J., Yanikomeroglu, H., Juntti, M., and Koucheryavy, Y. (2019). When iot keeps people in the loop: A path towards a new global utility. *IEEE Communications Magazine*, 57(1):114–121.

Peyrone, N. and Wichadakul, D. (2023). A formal model for blockchain-based consent management in data sharing. *Journal of Logical and Algebraic Methods in Programming*, page 100886.

Pilloni, V. (2018). How data will transform industrial processes: Crowdsensing, crowdsourcing and big data as pillars of industry 4.0. *Future Internet*, 10(3).

Pötzsch, S. (2009). Privacy awareness: A means to solve the privacy paradox? In Matyáš, V., Fischer-Hübner, S., Cvrček, D., and Švenda, P., editors, *The Future of Identity in the Information Society*, pages 226–236, Berlin, Heidelberg. Springer Berlin Heidelberg.

Pournajaf, L., Garcia-Ulloa, D. A., Xiong, L., and Sunderam, V. (2016). Participant privacy in mobile crowd sensing task management: A survey of methods and challenges. *SIGMOD Rec.*, 44(4):23–34.

Psychoula, I., Chen, L., and Chen, F. (2017). Privacy modelling and management for assisted living within smart homes. In *2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pages 1–6.

Purvis, B., Mao, Y., and Robinson, D. (2019). Three pillars of sustainability: in search of conceptual origins. *Sustainability Science*, 14(3):681–695.

Qi, M., Wang, Z., Han, Q.-L., Zhang, J., Chen, S., and Xiang, Y. (2022). Privacy protection for blockchain-based healthcare iot systems: A survey. *IEEE/CAA Journal of Automatica Sinica*, pages 1–20.

Ra, G., Kim, T., and Lee, I. (2021). Vaim: Verifiable anonymous identity management for human-centric security and privacy in the internet of things. *IEEE Access*, 9:75945–75960.

Rahman, M. S., Chamikara, M., Khalil, I., and Bouras, A. (2022). Blockchain-of-blockchains: An interoperable blockchain platform for ensuring iot data integrity in smart city. *Journal of Industrial Information Integration*, 30:100408.

Ramírez-Moreno, M. A., Keshtkar, S., Padilla-Reyes, D. A., Ramos-López, E., García-Martínez, M., Hernández-Luna, M. C., Mogro, A. E., Mahlknecht, J., Huertas, J. I., Peimbert-García, R. E., Ramírez-Mendoza, R. A., Mangini, A. M., Roccotelli, M., Pérez-Henríquez, B. L., Mukhopadhyay, S. C., and Lozoya-Santos, J. d. J. (2021). Sensors for sustainable smart cities: A review. *Applied Sciences*, 11(17).

Rantos, K., Drosatos, G., Demertzis, K., Ilioudis, C., Papanikolaou, A., and Kritsas, A. (2019). Advocate: A consent management platform for personal data processing in the iot using blockchain technology. In Lanet, J.-L. and Toma, C., editors, *Innovative Security Solutions for Information Technology and Communications*, pages 300–313, Cham. Springer International Publishing.

Rao, A., Schaub, F., Sadeh, N., Acquisti, A., and Kang, R. (2016). Expecting the unexpected: Understanding mismatched privacy expectations online. In *Proceedings of the Twelfth USENIX Conference on Usable Privacy and Security*, SOUPS '16, page 77–96, USA. USENIX Association.

Rashtian, H., Boshmaf, Y., Jaferian, P., and Beznosov, K. (2014). To befriend or not? a model of friend request acceptance on facebook. In *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security*, SOUPS '14, page 285–300, USA. USENIX Association.

Rho, S. and Chen, Y. (2018). Social internet of things: Applications, architectures and protocols. *Future Generation Computer Systems*, 82:667–668.

Rios, R., Onieva, J. A., Roman, R., and Lopez, J. (2022). Personal iot privacy control at the edge. *IEEE Security & Privacy*, 20(01):23–32.

Rivadeneira, J. E., Borges, G. A., Rodrigues, A., Boavida, F., and Silva, J. S. (2023a). A unified privacy preserving model with ai at the edge for human-in-the-loop cyber-physical systems. *Submitted to Internet of Things; Engineering Cyber Physical Human Systems*.

Rivadeneira, J. E., Filipe Pinto, M., and Sá Silva, J. (2020). A qualitative study on trust perception in iot mobile applications. In *2020 IEEE Colombian Conference on Communications and Computing (COLCOM)*, pages 1–6.

Rivadeneira, J. E., Jiménez, M. B., Marculescu, R., Rodrigues, A., Boavida, F., and Sá Silva, J. (2023b). A blockchain-based privacy-preserving model for consent and transparency in human-centered internet of things. In *Proceedings of the 8th ACM/IEEE Conference on Internet of Things Design and Implementation*, IoTDI '23, page 301–314, New York, NY, USA. Association for Computing Machinery.

Rivadeneira, J. E., Silva, J. S., Colomo-Palacios, R., Rodrigues, A., and Boavida, F. (2023c). User-centric privacy preserving models for a new era of the internet of things. *Journal of Network and Computer Applications*, page 103695.

Rivadeneira, J. E., Sá Silva, J., Colomo-Palacios, R., Rodrigues, A., Fernandes, J. M., and Boavida, F. (2021). A privacy-aware framework integration into a human-in-the-loop iot system. In *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 1–6.

Rivadeneira, J. E., Sánchez, O. T., Dias, M., Rodrigues, A., Boavida, F., and Silva, J. S. (2023d). Confluence: An integration model for human-in-the-loop iot privacy-preserving solutions towards sustainability in a smart city. *Submitted to IEEE Internet of Things Journal*.

Rodrigues, J. (2022). *Novos Modelos de Privacidade para a Internet das Coisas*. Msc thesis, University of Coimbra, DEEC.

Saha, S., Chattaraj, D., Bera, B., and Kumar Das, A. (2021). Consortium blockchain-enabled access control mechanism in edge computing based generic internet of things environment. *Transactions on Emerging Telecommunications Technologies*, 32(6):e3995.

Saha, S., Sutrala, A. K., Das, A. K., Kumar, N., and Rodrigues, J. J. P. C. (2020). On the design of blockchain-based access control protocol for iot-enabled healthcare applications. In *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pages 1–6.

Salinger, S., Plonka, L., and Prechelt, L. (2008). A coding scheme development methodology using grounded theory for qualitative analysis of pair programming. *Human Technology: An Interdisciplinary Journal on Humans in ICT Environments*.

Sanchez, O. T., Fernandes, J. M., Rodrigues, A., Silva, J. S., Boavida, F., Rivadeneira, J. E., de Lemos, A. V., and Raposo, D. (2022). Green bear - a lorawan-based human-in-the-loop case-study for sustainable cities. *Pervasive and Mobile Computing*, 87:101701.

Satybaldy, A. and Nowostawski, M. (2020). Review of techniques for privacy-preserving blockchain systems. In *Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure*, BSCI '20, page 1–9, New York, NY, USA. Association for Computing Machinery.

Seliem, M., Elgazzar, K., and Khalil, K. (2018). Towards privacy preserving iot environments: A survey. *Wireless Communications and Mobile Computing*, 2018.

Senarath, A., Arachchilage, N. A. G., and Slay, J. (2017). Designing privacy for you: A practical approach for user-centric privacy. In Tryfonas, T., editor, *Human Aspects of Information Security, Privacy and Trust*, pages 739–752, Cham. Springer International Publishing.

Shu, L., Chen, Y., Huo, Z., Bergmann, N., and Wang, L. (2017). When mobile crowd sensing meets traditional industry. *IEEE Access*, 5:15300–15307.

Silva, J. S., Zhang, P., Pering, T., Boavida, F., Hara, T., and Liebau, N. C. (2017). People-centric internet of things. *IEEE Communications Magazine*, 55(2):18–19.

Sinche, S., Hidalgo, P., Fernandes, J. M., Raposo, D., Silva, J. S., Rodrigues, A., Armando, N., and Boavida, F. (2020a). Analysis of student academic performance using human-in-the-loop cyber-physical systems. *Telecom*, 1(1):18–31.

Sinche, S., Raposo, D., Armando, N., Rodrigues, A., Boavida, F., Pereira, V., and Silva, J. S. (2020b). A survey of iot management protocols and frameworks. *IEEE Communications Surveys & Tutorials*, 22(2):1168–1190.

Smith, S. (2003). Humans in the loop: human-computer interaction and security. *IEEE Security & Privacy*, 1(3):75–79.

Sun, Y., Chen, S., Zhu, S., and Chen, Y. (2020). Iryp: A purely edge-based visual privacy-respecting system for mobile cameras. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '20, page 195–206, New York, NY, USA. Association for Computing Machinery.

Sutrala, A. K., Obaidat, M. S., Saha, S., Das, A. K., Alazab, M., and Park, Y. (2022). Authenticated key agreement scheme with user anonymity and untraceability for 5g-enabled softwarized industrial cyber-physical systems. *IEEE Transactions on Intelligent Transportation Systems*, 23(3):2316–2330.

Torre, I., Adorni, G., Koceva, F., and Sanchez, O. (2016a). Preventing disclosure of personal data in iot networks. In *2016 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*, pages 389–396.

Torre, I., Koceva, F., Sanchez, O. R., and Adorni, G. (2016b). A framework for personal data protection in the iot. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 384–391.

Torres, O., Dávila, G., Rivadeneira, J. E., and Hidalgo, P. (2020). A vulnerability analysis of the ieee 802.15.6 display authenticated association protocol. In *2020 IEEE Colombian Conference on Communications and Computing (COLCOM)*, pages 1–6.

Tsampoulatidis, I., Komninos, N., Syrmos, E., and Bechtsis, D. (2022). Universality and interoperability across smart city ecosystems. In Streitz, N. A. and Konomi, S., editors, *Distributed, Ambient and Pervasive Interactions. Smart Environments, Ecosystems, and Cities*, pages 218–230, Cham. Springer International Publishing.

Vergara-Laurens, I. J., Jaimes, L. G., and Labrador, M. A. (2017). Privacy-preserving mechanisms for crowdsensing: Survey and research challenges. *IEEE Internet of Things Journal*, 4(4):855–869.

Wagenaar, G., Overbeek, S., Lucassen, G., Brinkkemper, S., and Schneider, K. (2018). Working software over comprehensive documentation – rationales of agile teams for artefacts usage. *Journal of Software Engineering Research and Development*, 6(1):7.

Wang, D., Amin, M. T., Li, S., Abdelzaher, T., Kaplan, L., Gu, S., Pan, C., Liu, H., Aggarwal, C. C., Ganti, R., Wang, X., Mohapatra, P., Szymanski, B., and Le, H. (2014). Using humans as sensors: An estimation-theoretic perspective. In *IPSN-14 Proceedings of the 13th International Symposium on Information Processing in Sensor Networks*, pages 35–46.

Wang, D., Szymanski, B. K., Abdelzaher, T., Ji, H., and Kaplan, L. (2019a). The age of social sensing. *Computer*, 52(1):36–45.

Wang, X., Ning, Z., Zhou, M., Hu, X., Wang, L., Zhang, Y., Yu, F. R., and Hu, B. (2019b). Privacy-preserving content dissemination for vehicular social networks: Challenges and solutions. *IEEE Communications Surveys & Tutorials*, 21(2):1314–1345.

Wang, Y., Huang, Y., and Louis, C. (2013). Towards a framework for privacy-aware mobile crowdsourcing. In *2013 International Conference on Social Computing*, pages 454–459.

Wei, X., Zhao, J., Zhou, L., and Qian, Y. (2020). Broad reinforcement learning for supporting fast autonomous iot. *IEEE Internet of Things Journal*, 7(8):7010–7020.

Weng, J., Deng, R. H., Ding, X., Chu, C.-K., and Lai, J. (2009). Conditional proxy re-encryption secure against chosen-ciphertext attack. In *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, ASIACCS '09, page 322–332, New York, NY, USA. Association for Computing Machinery.

Wicker, S. B. and Schrader, D. E. (2011). Privacy-aware design principles for information networks. *Proceedings of the IEEE*, 99(2):330–350.

Wijesundara, A. (2020). Engineering privacy-aware smart home environments. In *Companion Proceedings of the 12th ACM SIGCHI Symposium on Engineering Interactive Computing Systems*, EICS '20 Companion, pages 1–3, New York, NY, USA. Association for Computing Machinery.

Wood, A. D. and Stankovic, J. A. (2008). Human in the loop: Distributed data streams for immersive cyber-physical systems. *SIGBED Rev.*, 5(1).

Worthy, P., Matthews, B., and Viller, S. (2016). Trust me: Doubts and concerns living with the internet of things. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*, DIS '16, page 427–434, New York, NY, USA. Association for Computing Machinery.

Xiao, R., Wu, Z., and Hamari, J. (2022). Internet-of-gamification: A review of literature on iot-enabled gamification for user engagement. *International Journal of Human–Computer Interaction*, 38(12):1113–1137.

Xu, C., Ren, J., Zhang, D., and Zhang, Y. (2018). Distilling at the edge: A local differential privacy obfuscation framework for iot data analytics. *IEEE Communications Magazine*, 56(8):20–25.

Xu, Q., Yu, C., Yuan, X., Fu, Z., and Liu, H. (2023). A privacy-preserving distributed subgradient algorithm for the economic dispatch problem in smart grid. *IEEE/CAA Journal of Automatica Sinica*, 10(7):1625–1627.

Xu, Z. and Zhu, S. (2015). Semadroid: A privacy-aware sensor management framework for smartphones. In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, pages 61–72.

Yang, Y., Zheng, X., Guo, W., Liu, X., and Chang, V. (2019). Privacy-preserving smart iot-based healthcare big data storage and self-adaptive access control system. *Information Sciences*, 479:567–592.

Yuan, D., Li, Q., Li, G., Wang, Q., and Ren, K. (2020). Priradar: A privacy-preserving framework for spatial crowdsourcing. *IEEE Transactions on Information Forensics and Security*, 15:299–314.

Zavalyshyn, I., Duarte, N. O., and Santos, N. (2018). Homepad: A privacy-aware smart hub for home environments. In *2018 IEEE/ACM Symposium on Edge Computing (SEC)*, pages 58–73.

Zhao, Y., Li, M., Lai, L., Suda, N., Civin, D., and Chandra, V. (2018). Federated learning with non-iid data. *arXiv*.

Zheng, S., Apthorpe, N., Chetty, M., and Feamster, N. (2018). User perceptions of smart home iot privacy. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW).

Zyskind, G., Nathan, O., and Pentland, A. S. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*, pages 180–184.