5-14-2018 10:45 AM

# Privacy-Protection in Cooperative Distributed Systems

Ali Saleh, *The University of Western Ontario*

Supervisor: Dr. Hamada Ghenniwa, *The University of Western Ontario*

A thesis submitted in partial fulfillment of the requirements for the Master of Engineering Science degree in Electrical and Computer Engineering

# Abstract

The new form of digital computational capabilities and internet connectivity continuous to grow. And introduce a new form of computation that is emerging rapidly with cloud computing, mobile computing, wearable computing and the Internet-of-Things.

All can be characterized as a class of "Cooperative Distributed Systems" (CDS) in the *open environment*. A major drive of the growth involves massive number of people and organizations, that have been engaged within their all daily life. In this context, users' privacy protection has become an essential requirement beyond the traditional approaches. This change requires a formal treatment of "privacy concern" as a fundamental computation concept in CDS paradigm.

The objective of this work is to develop a model for "privacy protection" as a foundation to build a CDS based framework and platform in which various applications allow users to enjoy the comprehensive services in open environments while protecting their privacy. The framework has been measured from an *Efficiency* and *Feasibility* aspect. To this end, formal foundation and model of privacy concern has been treated in the aspect of information management. This proposed framework serves as a base for a practical privacy protection management in CDS. It includes a privacy-aware agent model and privacy-based platform for CDS with the ability to support interaction-based privacy protection.

The practical aspects of the proposed framework have been demonstrated by developing an Interaction-based CDS computational platform.

## Keywords

Cooperative Distributed System (CDS), Interaction, Privacy Protection, Information Categorization, Practical Computation Platform.

# *Acknowledgments*

This work would not have been done without the unlimited support from my main supervisor, research team and family.

First and foremost, all praise is due to Allah, the Beneficent, the Merciful. He has guided me; given me the potential, and without his blessings I would not be able to make this degree possible.

In the course of my Master’s degree I would like to show my sincerest appreciation and gratefulness to my supervisor professor. Ghenniwa, Hamada, for the great fortune of being supervised by a very supportive and helpful supervisor. His integrity, dedication, insightful advice and encouragement have greatly contributed in fulfilling this degree and giving me the opportunity to be involved in such learning experience.

I would also like to thank my research group members the CDS-Eng group for all their constructive comments and suggestions which surely helped in improving the thesis at the Department of Computer and Electrical Engineering for their constant efforts and willingness to help.

I remain indebted and grateful to my parents for their prayers, both of whom have always believed in me; my brothers, sisters, and friends for their continuous support.

Last, but certainly not least, I would like to express my sincere gratitude to my beloved country Libya for investing in me and give me the opportunity to enhance my academia level by all the financial and the professional follow-up and management of my scholarship during my study journey.

# Table of Contents

Abstract ........ i

Acknowledgments ........ ii

Table of Contents ........ iii

List of Figures ........ vii

Symbols and Notations ........ ix

Chapter 1 ........ 1

1 Introduction ........ 1

1.1 Cooperative Distributed System and Privacy Concerns ........ 1

1.2 Privacy: Concepts, Issues and Models ........ 4

1.3 Scope of the thesis ........ 6

1.3.1 Practical Privacy Model ........ 7

1.3.2 Practical Privacy Protection Management Framework ........ 8

1.3.3 Privacy-Aware Computation Platform ........ 9

1.4 Organization of Thesis ........ 11

Chapter 2 ........ 12

2 Background and Literature Review ........ 12

2.1 Privacy Protection by The Law ........ 12

2.2 Privacy Protection in Information Management ........ 16

2.2.1 Personal Identifiable Information (PII) ........ 17

2.3 Privacy in Distributed Systems ........ 19

2.3.1 Privacy and Security in Authorization Framework ........ 19

2.3.2 Privacy Protection in Multiple Data Sources ........ 20

2.3.3 Privacy in Distributed Constraint Satisfaction ........ 21

2.4 Privacy in Distributed Artificial Intelligence ........ 23

2.5 Privacy Protection in Cooperative Distributed Systems ........................................... 24

2.5.1 Privacy in Auction Mechanisms ............................................................ 24

2.5.2 Risk Analysis ............................................................................................ 25

2.5.3 Targeting Advertisement ....................................................................... 26

2.5.4 Privacy Protection Management in CDS ................................................ 27

2.6 Summary ......................................................................................................... 28

Chapter 3 ............................................................................................................ 29

3 Privacy Concerns in CDS: Concepts and Models ....................................... 29

3.1 CDS: An Agent-based Model ........................................................................ 29

3.2 Privacy Concern Analysis and Model ........................................................ 31

3.3 Privacy Concerns Management ................................................................... 36

3.4 Privacy Protection in CDS ............................................................................ 38

3.4.1 Privacy Protection Mechanism ............................................................... 40

Chapter 4 ............................................................................................................ 45

4 Privacy Protection Management Framework ............................................. 45

4.1 Privacy Protection at the Interaction Level ............................................... 45

4.1.1 Privacy-Based Interaction Protocol ........................................................ 46

4.2 Privacy Protection at the Interaction Level ............................................... 48

Chapter 5 ............................................................................................................ 53

5 Privacy Protection Model and Practical Implementation ........................... 53

5.1 Privacy Protection Concept at the Interaction Level ................................ 53

5.2 Privacy Protection Management Framework in CDS ................................ 56

5.2.1 Information Sensitivity Categorization .................................................... 57

5.2.2 Exposure Boundary Identification .......................................................... 61

5.2.3 Privacy- Based Interaction protocol ........................................................ 66

5.2.3.1 Privacy Protection-Based Interaction Protocol Termination ...... 69

5.2.3.2 Privacy Protection Interaction Protocol Outcome ...................... 70

5.2.3.3 Privacy Protection Interaction Protocol Practicality Analysis ... 71

5.3 Practical Privacy Protection Computation Based ..................................................... 74

5.4 Privacy Protection as an Architecture Computation. ................................................ 75

5.4.1 Communication and Computational Complexity .................................... 77

5.4.2 Computation Architecture Implementation ............................................. 82

5.5 Summary ........................................................................................................... 84

Chapter 6 .............................................................................................................. 85

6 Privacy Protection Platform in CDS Model: Application Scenarios ........................... 85

6.1 Smart Space Project ........................................................................................... 85

6.2 Privacy concerns and protection in Smart Space ...................................................... 89

6.2.1 Privacy Concern Scenarios ....................................................................... 90

6.2.2 Privacy Protection Platform based. .......................................................... 91

6.3 Summary ........................................................................................................... 94

Chapter 7 .............................................................................................................. 95

7 Privacy Protection-Based Implementation.................................................................. 95

7.1 Experimental setup ............................................................................................. 95

7.1.1 Architecture Level ..................................................................................... 95

7.1.2 Deployment Level...................................................................................... 97

7.1.3 Design Principle on Privacy Concerns .................................................... 98

7.2 Detailed Design and Implementation ........................................................................ 99

Chapter 8 .............................................................................................................. 106

8 Conclusion and Future Work ........................................................................... 106

8.1 Contributions summary ........................................................................................ 106

8.1.1 Challenge and Contributions.................................................................. 106

8.2 Future Work...................................................................................................... 108

References.......................................................................................................................

Curriculum Vitae ..............................................................................................................

# List of Figures

Figure 1. Growth of ‘things’ connected to the Internet .......................................................... 2

Figure 2: Computation Entity in CDS ..................................................................... 30

Figure 3: Privacy Protection at the Interaction Level ........................................................... 55

Figure 4: Information Categorization ...................................................................... 60

Figure 5: Privacy protection aware entity ................................................................... 62

Figure 6  Information Exposure Boundary Identification ...................................................... 65

Figure 7. Information Categorization Management Engine .................................................. 66

Figure 8: Interaction among entities in open environment .................................................... 77

Figure 9: Mediator architecture in open environment ........................................................... 78

Figure 10: Privacy Protection Base Platform ........................................................................ 79

Figure 11: Privacy Protection based Platform ...................................................................... 81

Figure 12: Privacy protection based computational platform ................................................ 83

Figure 13: Privacy Protection Aware Entity .......................................................................... 84

Figure 14: CIR- Smart Object Logical Architecture ............................................................. 86

Figure 15: Mapping the Smart Object to CIR-Agent ............................................................ 86

Figure 16:  Smart object privacy-based interaction device .................................................... 88

Figure 17: Computational Engagement Platform "DEXIT" .................................................. 89

Figure 18 Smart Object Privacy Protection Aware ................................................................ 92

Figure 19: Computational Privacy Based Engagement Platform ........................................... 93

Figure 20: System Architecture ........................................................................................ 96

Figure 21: Deployment Architecture ................................................................................ 97

Figure 22: Privacy Protection-Based Interaction Protocol ..................................................... 99

Figure 23: Service registration at the platform ..................................................................... 100

Figure 24: Service broker registration ..................................................................................... 101

Figure 25:  Requester smart object ......................................................................................... 102

Figure 26: Encrypt and Decrypt Service.................................................................................. 104

# Symbols and Notations

The following is the list of symbols and notation frequently used in this work.

| **Notation/Symbol** | **Concept** |
|---|---|
| $E$ | Environment is a CDS-based space where does entities exist |
| $\mathrm{e}_{\mathrm{i}}$ | A computation entity in CDS environment<br>i: is the entity identity |
| $\mathrm{I}_{\mathrm{i}}$ | Set of information that is owned by $e_i$<br>i: is the entity identity |
| $O_{\mathrm{i}}$ | Set of operations that is owned by $e_i$<br>i: is the entity identity |
| $E_{i,k}$ | Exposure Boundary of $\mathrm{I}_{\mathrm{i,k}}$ that includes entities for which sharing $\mathrm{I}_{\mathrm{i,k}}$ can take place without causing privacy concern.<br>i: is the entity identity<br>k: is the information identifier |
| $I^S(I_{i,k}, \mathrm{e}_{\mathrm{j}})$ | $I_{i,k}$ is Sensitive in relation with $\mathrm{e}_{\mathrm{j}}$ from $\mathrm{e}_{\mathrm{i}}$ perspective<br>i: is the entity identity that owns the information<br>j: is the entity identifier that does not belong to $E_{i,k}$<br>k: is the information identifier |
| $\bar{\bar{o}}(\mathrm{I}^{\mathrm{exp}}, \mathrm{I}^{\mathrm{Shar}}, \mathrm{I}^{\mathrm{imp}})$ | Executing Operation $(\mathrm{o})$ on explicit information $\mathrm{I}^{\mathrm{exp}}$ to transform the implicit information to explicit form of $\mathrm{I}^{\mathrm{imp}}$ |
| $\bar{\bar{o}}(\mathrm{I}^{\widetilde{\mathrm{x1}}, \widetilde{\mathrm{I}}\mathrm{aux}})$ | Preventing/Neutralizing Execution of operation $(o)$ on $\mathrm{I}^{\mathrm{x1}}$ given the auxiliary information $\mathrm{I}^{\mathrm{aux}}$ |
| $\mathrm{S}(\mathrm{I}_{\mathrm{i,k}}, \mathrm{e}_{\mathrm{j}})$ | Sharing $\mathrm{I}_{\mathrm{i,k}}$ with $\mathrm{e}_{\mathrm{j}}$<br>i: is the entity identifier that owns the information<br>j: is the entity identifier that receives $\mathrm{I}_{\mathrm{i,k}}$<br>k: is the information identifier |
| $\mathrm{D}(\mathrm{I}_{\mathrm{i,k}}, \mathrm{e}_{\mathrm{j}})$ | Disclosure of $\mathrm{I}_{\mathrm{i,k}}$ to $\mathrm{e}_{\mathrm{j}}$<br>i: is the entity identifier that owns the information<br>j: is the entity identifier that $\mathrm{I}_{\mathrm{i,k}}$ is disclosed to<br>k: is the information identifier |
| $\hat{O}_j^{i,k}$ | Non-Authorized operations in $O_j$ that can be applied on $\mathrm{I}_{\mathrm{i,k}}$<br>i: is the entity identifier that owns the information |

| | |
|---|---|
| | j: is the entity identifier that $\mathrm{I}_{\mathrm{i,k}}$ is disclosed to |
| | k: is the information identifier |
| $\hat{O}_j^i$ | All possible non-authorized operations in relation with $\mathrm{e}_\mathrm{j}$ |
| | i: is the entity identifier that owns the information |
| | j: is the entity identifier that can receive information from $e_i$ |
| $\mathrm{PV}\left(\mathrm{e}_\mathrm{j}, \mathrm{I}_{\mathrm{i,k}}, \hat{\mathrm{O}}_\mathrm{j}^{\mathrm{i,k}}, \theta_{i,j}^{i,k}\right)$ | Privacy Violation of $\mathrm{e}_\mathrm{i}$ by $\mathrm{e}_\mathrm{j}$ disobeying the agreement $\theta_{\mathrm{i,j}}$ between $\mathrm{e}_\mathrm{i}$ and $\mathrm{e}_\mathrm{j}$ by executing a non-authorized operations belonging to $\hat{\mathrm{O}}_\mathrm{j}^{\mathrm{i,k}}$ on $\mathrm{I}_{\mathrm{i,k}}$ |
| $\mathrm{PP}\left(\mathrm{e}_\mathrm{j}, \left(\mathrm{PS}(\mathrm{I}_\mathrm{i})\right), \hat{O}_j\right)$ | Privacy protection of $\mathrm{e}_\mathrm{i}$ when $\mathrm{I}_\mathrm{i}$ is the space and $\hat{O}_j$ is all possible non-authorized operations in $\mathrm{e}_\mathrm{j}$ |
| $\mu$ | Privacy Protection Mechanism |
| $\bar{\bar{\mu}}$ | Applying privacy protection mechanism |
| $\mathrm{PPL}(\mathrm{e}_\mathrm{j}, \mathrm{I}_\mathrm{i}, \mu)$ | PPL: probability of privacy protection of $\mathrm{e}_i$using $\mu$ protection mechanism in interaction with $\mathrm{e}_\mathrm{j}$ |
| $IP$ | Interaction protocol |
| $R^*$ | Participating Entities in an interaction protocol |
| $I_i^s$ | All sensitive information in $\mathrm{e}_i$ in relationship with entities in $R^*$ |
| $S_M$ | Sequences of messages in an interaction protocol |
| $ss_{q,t}$ | Sub-sequences of a sequence |
| | q: Sequence identifier |
| | t: sub-sequence identifier |
| $ss_{q,t}^o$ | All operations of a sub-sequence |
| | q: Sequence identifier |
| | t: sub-sequence identifier |
| $\bar{\bar{ss}}_{q,t}^o(M)$ | Execution of operations of a subsequence |
| | q: Sequence identifier |
| | t: sub-sequence identifier |
| $\mu_{i,k}$ | Protection Operation in a computation entity that is applied for protecting $I_{i,k}$ that is classified as sensitive |

# Chapter 1

# 1 Introduction

The computing innovation has been rapidly accelerated over the last decade. The computation has evaluated from colossal machines to the ever-present digital era that is characterized by technologies that involves a massive number of people and organizations. In this new era of technology has engaged a vast number of smart objects and its applications in the new area of computation known as Internet-of-Things (IoT).

Consciously, a significant part of human life will be exposed and coxswained by computation systems. This raise the flag of the privacy concern of individuals personal information privacy that might reveals the extent of which there could be a risk to privacy concerns. The personal information privacy has been introduced in different areas and investigated from many different aspects. The focus in this chapter the privacy model, and its' issues and model has been demonstrated and how they the privacy protection has been formally modeled.

## 1.1 Cooperative Distributed System and Privacy Concerns

In the new computation evolution more entities increasingly interconnected, intricate and quickly changing world. People and businesses are engaging with various applications and because of this, it is envisioned that a significant part of our lives will be steered by computation systems in near future. According to the survey that has been done by Cisco [25] they have predicted that 50 billion new internet-connected will be made in IoT by 2020 as a result of a major advancement in Information and Communication Technology. Figure 1. Growth of 'things' connected to the Internet shows that, in 2008 the number of the interconnected entities that are equipped with internet connectivity surpassed the population globally [71]. The development of computation environments that delivering services to people and businesses, the privacy become a major challenge in such environments [68], [10].

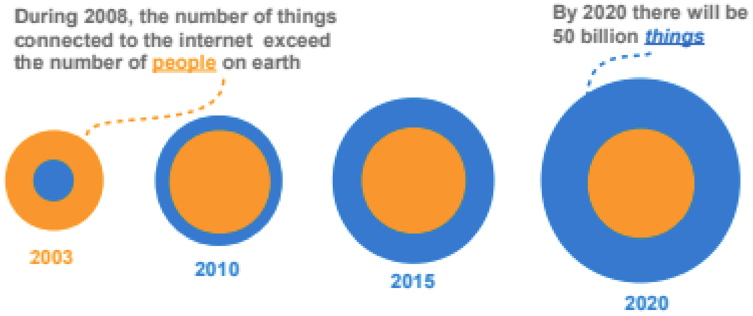


**Figure 1. Growth of ‘things’ connected to the Internet**

The evolution of the Distributed Systems has introduced a form of computation that steered the involvement and the significant impact of the information technology on people's daily lives which is the Cooperative Distributed Systems (CDS).

CDS is an important class of distributed systems. Where it is consisting of entities that are able to exercise a degree of authority in sharing their capabilities. This characteristic is very desirable in designing systems for many applications domains, such as learning, manufacturing engineering and virtual environments. In CDS, entities are autonomous self-interested interact on behalf of their principals. Entities exercise some degree of authority in share their capabilities and require the computation capability of other entities in the environment to help them to achieve their goal. In the process of interaction and engaging, information exchange among participant entities. The exchanged information is collected by many processes and devices and hence has brought increased risks regarding the concerns on one’s privacy. Information about people is gathered through many service providers, stored in various infrastructures, analyzed and reported for further objectives [7]. In such, the information is manipulated towards extracting and disseminating the information to other parties or serving various interests [14]. In particular, in open environments, it would be a strong assumption that entities in the environment will have a degree of respect for the privacy of others.

Open environment refers to environments that consist of various autonomous self-interested entities which have each of the entities is capable to exercises a capability of achieving a service. In the open environment there are no global knowledge about who does exist, what are their capability, and when and where they do exist. Since they have the capability over their activity then they are dynamically participant.

The computation in distributed heterogeneous environments that are modeled as CDS occurs during interaction between entities, where the information is shared. This entails capturing privacy at the computation level [7]. This view is contrary to the traditional approaches towards privacy through which the application filters the computation solutions based on predefined rules [6],[37]. The privacy models can be classified into two main categories: rule-based approaches and architectural-based approaches [10]. Privacy solution models that evolve from rule-based approaches are typically designed for stable, low variant environments such as Privacy Policy for Social Networks. These approaches mainly concentrate on applying rules onto information that is collected during the process of sharing. Due to the open environment assumption in many applications of CDS, the rule-based approaches [18] are not sufficient [10],[70]. Information processing has been the engine of extracting information by applying operations on it. This information is not necessarily captured in rule-based privacy models. Furthermore, since the rules and policies can impose limitation of the design and dynamism of the environments, many open CDS environments cannot adopt these perspectives on privacy.

Among architectural-based privacy solutions are anonymization techniques [8][14][16], privacy utility trade off mechanisms, [7] , [74] , social tradeoffs and proxy-based privacy protection [66]. In this context, the anonymization techniques are limited to particular settings that include a trusted information collector entity and non-continuous information dissemination processes that are not adequate for open CDS environments [19]. The work in [39] illustrates that privacy utility trade off models do not necessarily reflect the preferences that each entity might have over their privacy. The utility tradeoff mechanisms have been applied in contexts such as smart power grid in which privacy is reduced to limited access to individualized signal from the aggregated view of the collected signal [62]. These models also evolved with approaches for measuring the risk of privacy concerns. Such risk adheres to the execution of operations that causes privacy concern, but it can measure the probability of the entity’s information being used [9] . In all cases, the limitation of the proposed models indicates the lack of adequate privacy model for CDS.

It is noteworthy that privacy is correlated with the interaction aspects of computation systems. This asserts that privacy is a computation concept that is related to the interaction process and can be adequately addressed by interaction protocols. For instance, if a specific entity can reach solution by acquiring the capabilities of entity the devised interaction protocol for such engagement has to coordinate the pertinent activities with However, during this engagement, may exploit the information as part of the messages in the interaction protocol and thus could result in privacy concern for. Capturing privacy as a concept in interactions still adheres to the mechanism of interaction as well as finding solutions that may not be conducive to privacy concerns for the participant entities.

## 1.2 Privacy: Concepts, Issues and Models

Privacy is an ethical, a social and a legal concept that has gained in many various definitions. Merriam-Webster Dictionary defines privacy as “the state of being alone: the state of being away from other people” while the Oxford Dictionary defines it as “the state in which one is not observed or disturbed by other people”. In all definitions, privacy becomes an inherent aspect of an environment of multiple people (entities/agents) or a setting of decentralized entities/agents.

Privacy protection is an essential and desirable aspect of CDS in open environment. The privacy protection is modeled as the prevention or neutralization of non-authorized operations execution on information. In an information management model of computation, “privacy” contains some specific connotations though in many ways the term is similar to how it is generally understood. In communication-based interaction among entities becomes a privacy concern when *sensitive* information flows outside the entity or the unit of entities in CDS. Evidently, it will be a more difficult challenge in CDS in particular when communication-based interactions are applied in open environments.

Motivated by the computational view on privacy, understanding privacy concept that can be applied in contexts such as CDS requires formal analysis of privacy. The work in [71] they have introduced formal foundations and model of privacy is developed within the context of information management. This served as a base for developing a privacy protection management framework for CDS. It includes a privacy-aware agent model for CDS platform with the ability to support interaction-based privacy protection. In another work in [54] proposes a formal approach for capturing privacy in information management in the context of social networks. However, the analysis stays at formulating the norms and relationship of the roles, and the concept of privacy is not clearly stated. In addition, the concept of norms and contexts can be implicit and exist in gray areas when it comes to social networks [21]. Also, in [56] they have addressed a major challenge of brokering in open environments is to support privacy. Within the context of brokering, privacy is modeled in terms of the entities’ ability. Different approaches of privacy models have been proposed to deal with relevant privacy issues [20][27][37]. However; to our knowledge, none of these approaches have treated and captured privacy at the computational level adequate for the CDS environments.

There have been significant efforts towards building a foundation for privacy rights during digital interactions. This enables an understanding of privacy and adopting the associated concepts based on practices in information technology law [22][23]. Many countries have enacted laws and legislations to protect people’s privacy. For instance, the Canadian law has several legal acts that oblige service providers and consumers to be responsible on respecting privacy as a right for people. Canadian Information Privacy Act and Access to information are among these legal supports. Furthermore, some privacy models were motivated by the supporting legal scenarios and rules [5]. Due to limitations on the setting of the rules and scenarios, employing these models impose *closed* assumption on the environment.

## 1.3 Scope of the thesis

A key objective of this work is to conduct a deep analysis of “privacy” and to develop a privacy protection model and computation concepts of privacy concerns. For this reason, this dissertation utilizes the formal model to extend the privacy protection framework for CDS-based applications [71] because of the need for a practical privacy protection solution that can carry on the privacy concern in the open environment where the participant entities are not predictable and are not predefined.

In many cases privacy is studied and treated in conjunction or within the context of “security” and “trust”. Although practically these concepts might be directly related, within this thesis, however, our focus is on analyzing the foundation of privacy and developing a fundamental model as computation concept in the CDS paradigm. Our belief is privacy is an intrinsic concept. In this work, privacy is viewed within the context of managing information manipulation, in particular “sensitive” information, within a given exposure boundary, for given security and trust measurements. In this respect, “security” mechanisms are concerned with the truthfulness of the communication within the areas of confidentiality, integration and availability, and “trust” is defined as degree of belief of reliability among entities in a particular context. This direction makes the principle foundations of our findings expandable to model and address situations where security and trust are involved.

Additionally, the major contribution of this work is its focus on the practicality aspects of the privacy protection framework for open environments. The main target indifferent perspectives to study and analyze the privacy protection management framework [71] from a different perspective. The focus in this work is to handle the practical aspects of the framework principles in terms of feasibility and efficiency.

This framework is applied in the Content Net Protocol (CNP) interaction protocol, which captures all the privacy concern aspects that can arise during the interaction and transforms the interaction protocol into a privacy-based interaction protocol. The practicality of the framework when applying the CNP interaction protocol needs to be considered to maintain the original behavior of the interaction protocol after the privacy protection mechanisms extension. However, in this work the original interaction operation of the interaction protocol has not been substituted. Yet, the operation of the interaction protocol has only been extended with privacy protection operations.

### 1.3.1Practical Privacy Model

The formal privacy model that is applicable for a CDS [71] was the motivation to extend it and develop a formal practical treatment of privacy for CDS environments. The proposed model is used as an analytical tool to evaluate the state of privacy during any entity's interaction.

Entities discern their sensitivity of information differently, depends on the recipients of the information during the interaction. Sensitive information perceived in relation to one entity might be considered totally non-sensitive to another. Entities tend to not *share* information when it is labeled as sensitive. This creates an exposure boundary for entities' information, which positions privacy as the state of the exposure boundary of the information. Information within the exposure boundary is non-sensitive but becomes sensitive when it exists outside of the exposure boundary.

Information exists in explicit forms. However, it can be classified as implicit information when it is in conjunction with operations. Operations can retrieve explicit information by processing the said information. The execution of operations transforms the implicit information to an explicit form. Through this transformation information might be transferred to outside of the exposure boundary therefore become sensitive. This implies that the concern with privacy is about the *disclosure* of sensitive implicit information. For example, various IaaS (Infrastructure as a Service) [17][31] providers serve their consumers by offering them resources, including memory, storage, and computational power, among others. In many forms of IaaS service delivery models, payment packages (pay per user) are based on the demands of entities. When the provider is not serving a higher priority consumer, economical packages receive response from the server. The advantage of costly packages is the guarantee of service at any time. Hence, serving an economical plan at the server implicitly implies not having a high priority job. Sharing scheduling information may enable an entity with a medium priority and resource-demanding job to acquire the service provider. Frequent preemption for lower priority consumers may lead to service blocking. This scenario explains that *sharing* the schedule is *not sensitive* when in possession of the scheduler, but it is *sensitive* whenever shared with other consumer entities.

In this work, we have provided a practical extension to the original privacy model that formally captures the concepts and concerns about privacy. Within this model, privacy concerns, privacy violation and privacy protection are formally explained and the necessary concepts to develop a framework for privacy protection management are introduced.

### 1.3.2 Practical Privacy Protection Management Framework

By employing the proposed privacy model, we established a practical privacy protection management framework that incorporates privacy protection mechanisms at the interaction level. Achieving a perfect privacy protection requires a complete knowledge about the environment. This complete knowledge cannot be attained in open environment since the is no global knowledge about the existence of other entities. We incorporated a quasi-protection mechanism that can protect privacy with a certain level of probability that is addressed as Privacy Protection Level (PPL) [71].

The framework captures the information of entities and accordingly evaluates the exposure boundaries associated to information. Consequently, it identifies the sensitive information and determines the necessary extension form for privacy protection. Using the PPL measure of each mechanism, the PPL of the privacy-based interaction protocol is evaluated and this enables applications to adopt privacy mechanisms that generate an acceptable level of PPL at the interaction level. It is proven in this work that this protection can sufficiently assist at the interaction level.

### 1.3.3 Privacy-Aware Computation Platform

Capturing privacy protection at the computation platform, will reduces the available solution choices to those entities that can fulfill the expected privacy requirements. The quantifiable model for the privacy concept allows for filtering the solutions space based on the privacy protection measures.

Match works has been devoted to the perspectives of authorization and rule management within underlying infrastructures [6][17]; privacy related concepts and the challenge with new technologies [5], taxonomy of privacy affairs [24], [70], privacy categorization and personally identifiable information [10]; and privacy within the context of information management, including information collection, information processing and information dissemination [26][34][35]. There also have been some attempts to formalize the languages used for privacy policies [5]. The economic mechanisms have been applied in this area as well with the objective of developing strategies through which privacy protection can be a dominant strategy [13]. Furthermore, privacy has been a main concern of multi-agent systems. Agents interact on behalf of their principals, engage in a number of activities and exchange information, which inevitably raises issues and concerns with regard to privacy [19].

Our research has contributed to several aspects of these areas, including sharing with privacy in information management, formalizing privacy concepts, personally identifiable information, privacy concepts and categorization and privacy within multi-agent systems and practical implementation in open environments. This work introduces a practical privacy-aware computation in open Cooperative Distributed Systems that addresses and manages privacy at the interaction level. The work also introduces several new original and novel ideas that contribute to the overall thesis that can be listed as follows:

**1) Privacy Model Implementation in the Context of Information Management**

A privacy concepts analysis is essential to capturing privacy as a computation concept. In this work, we have investigated privacy protection within the context of information management and sensitive information. Our attempts in understanding privacy in this context have resulted in developing a formal model that delivers a complete view of privacy protection in information management.

**2) Sensitive Information Privacy Management Interaction-Based Engine**.

Considering the incomplete knowledge of entities in open CDS environments, privacy protection is encountered with different uncertainty levels. To deal with this uncertainty, a probability-based model and utility-based model are applied. The information privacy protection management engine, which is based on the privacy protection management framework, enables managing the expected level of privacy protection within the interactions of entities. The proposed solution for practical protection of privacy has been congregated within an architectural approach towards an interaction-based framework for privacy protection in which the privacy protection mechanisms are applied to interactions as required.

**3) Practical Privacy as a Computation Concept**.

The privacy concept is practically treated at the interaction level by including privacy in the computation solution. As a result, the computation has been practically applied at two levels, partially adopted at as part of the computation entity architecture as well in the computation platform architecture.

### 4) Privacy-Based Interaction Protocol

Applying a privacy protection management framework to the interaction protocols allows for the identification if privacy concerns in those interactions. The proposed framework evaluates the messages and sequences of the interaction protocol and provides adequate protection operations within the interaction protocol that result in a privacy-based interaction protocol. The extended privacy-based interaction protocol that is generated by applying the privacy protection management framework can practically provide privacy protection in situations where knowledge of an entity in the CDS environment is incomplete. One of the interaction protocols that is utilized within this framework is Contract Net protocol (CNP). CNP is a negotiation-based interaction protocol that is designed for distributed problem solving. Due to privacy concerns in this protocol, we have applied the privacy protection management framework, which resulted in a privacy-based Contract Net interaction protocol.

## 1.4 Organization of Thesis

The rest of this work is organized as follows: Chapter 2 provides an overview of privacy in different areas of research. Chapter 3 provides a privacy concern in CDS as a concept, modeling and management. Subsequently, Chapter 4 proposes a practical privacy protection management framework. Chapter 5 elaborates on privacy protection aware model and practical implementation, as well as implementation challenges. Chapter 6 presents the privacy protection platform in the CDS model: application scenarios. Chapter 8 includes future work and the conclusion of this work is outlined.

# Chapter 2

# 2 Background and Literature Review

The objective in this part is to conduct a literature review and discuss the existing approaches, research methodology and challenges for protecting privacy issues with a special focus on implementation practicality associated with Cooperative Distributed Systems in open environments. These numerous applications allow users to take advantage of comprehensive services in open environments while protecting their privacy seamlessly. The more engagements that take place in digital developments, the more privacy concerns that occur. Based on the findings we will analyze and reflect on some of existing approaches the deal with privacy concern in CDS. We will compare the results of each of the papers and how this works can be related to our main research goal. Many disciplines have addressed privacy in their solutions. However, an adequate privacy models for CDS environments are still a challenge.

## 2.1 Privacy Protection by The Law

Text Privacy is a multi-disciplinary concept that is mainly tented within Law researches and legal schemes. Understanding privacy from the perspective of law enables us to observe and perceive privacy concerns in the context of information management. There are various views about privacy among different categories of law. One believes privacy is the product of the modern life where gossips became curiosity while another claim that privacy is as old as common law [22]. The work in [61] indicates that privacy is often interpreted as security and it is traded in return for providing security for the society or individual [23]. The concept of privacy has been studied in four main categories [22]:

- Common Law
- Constitutional Law

- Statutory Law
- International Law

Due to dynamic context of privacy, challenge in front of legal scholars is defining privacy rights which, in many cases are typically abstract and vague [22]. Researchers in legal areas try to retrieve the potentials of the existing law to propose solutions for protecting privacy and evaluate Law responses to new subjects such as privacy rights. Traditionally, privacy was treated as "decisional privacy" which mainly concerns the liberty of decisions about one's body and family. Nonetheless, because of the role of technology in spreading information about people and organizations and the direct effect of privacy in ones' lives, it has become the priority in legislative agenda in Congresses. History of privacy rights indicates multiple stories about people and organizations in which dissemination of information can directly target individuals' lives [22].

One of the main achievements in Privacy Law is presenting it as one's "Rights". The main issue in the current technology is the presence of medias that are utilized for circulating information. Such trend increases the effect of privacy in people's lives. Therefore, attorneys typically address privacy rights in the area of "common law". The objective is to protect privacy of private lives form unwanted intrusion. Accordingly, there are four type of intrusion in interaction of people and society [22]:

1. Intrusion upon seclusion and solitude.
2. Public disclosure of embarrassing private facts.
3. Publicity which exposes people in a false light in public.
4. Appropriation for people's interests.

As people's lives are now virtually available among various type of services and data sources, it would become essential for these services to adapt their solution in alignment with common law. However, privacy rights are not limited to common law and people's private life. More importantly, privacy concerns are not only about people. It can also be applied on how machines and software interact which can be addressed in information privacy. In this section, we try to extract the necessary foundation for privacy interactions so that we can associate them in general interaction among entities in CDS.

In attempt to identify the interactions that result in privacy violation from law perspective, four types of violation categories are presented above. Each of which can represent various circumstances that individuals or machines confront in open environments. For instance, the first category asserts on respecting people's solitude and private avocations. This implies that the actions performed by an entity in its private life are being monitored by another entity apart from their awareness. This is equivalent to the privacy concerns related to "information collection" and "information processing". Currently, digital life is an inseparable part of individuals' activities [22]. However, mainly, all the individual's online private affairs and activities are usually monitored and recorded by service providers. Software and machines are installed in many locations to observe and analyze human interactions. The motivations supporting these systems are tailored to improving business, security, better consumer support, safety, efficiency and many human perspectives. Yet, such motivations have brought about and created a tremendous challenge related to privacy in Cyberspace. Nonetheless, legal efforts are directed to finding solutions that can mitigate the issue by eliminating unnecessary monitoring and controlling tasks. The second Category implies the concern of public exposure of information, which might cause humiliation and embarrassments for individuals [22]. This is due to the *sharing* an individual's information to others without having the necessary consent. This form of privacy concerns is referred as secondary use whenever a third party is involved. With the explosion of Internet Media and personal pages in various web sites, individuals experience levels of disconcertion when their information is used in other contexts. Personal information is excessively spreading among Internet services and in noticeable amount of cases; it has been disseminated to other providers or publicly exposed.

Similar to the second category, the third category of intrusion occurs when disclosing false information entails the attraction of unnecessary attention to individuals [22]. Suppose in a reputation system built for auctions, an entity gets false negative feedback; it is without doubt that such falsification impact further future activities with this entity. Spreading false information about capabilities and availability of a service provider in a grid environment can forge the scheduling mechanism and hence may overload a provider or disrupt the whole scheduling system.

The last category of intrusion discusses the appropriation of exposing individuals' interest information [22]. Due to the possibility of extracting personal information about people by processing their interests in various subjects, interest information become sensitive. Given the growth of targeting advertisement, interest information is valuable to advertisers. This could exhibit levels of privacy concerns when the interest information is not appropriate.

As argued in [22], the challenge in investigating privacy violation is distinguishing the discussed aforementioned categories. For simplicity, they are addresses respectively as 1) intrusion, 2) disclosure, 3) false light and 4) appropriation. In spite of the similarity among these categories, they have characteristics that assist in separating the concepts. For instance, in intrusion and disclosure, existence of secret information is part of the scenario. In disclosure and false light, the publicity is the main element. However, in false light, falsified information or fiction differentiates it from disclosure. Appropriation typically involves in providing advantages for the owner of information [22].

Borrowing the intrusion categories in common low, similar concerns exist in cyber space. Among them are: “Breach of Confidentiality”, “Defamation”, “Infliction of emotional distress”, “privacy of home” [22] and “privacy in computing technology”.

Breach of Confidentiality”: this term commonly is used to define the revealing of patients' and client's information [22]. In this context, the patient is the consumer entity and the doctor is the service provider. If the service provider breaches the confidentiality of the information, it has disseminated the information to a third party without having the consent of the consumer.

Defamation refers to disrupting individuals' reputation by false information [22], where infliction of emotional distress is related to the emotional discomfort that individuals experience when their sensitive information is *shared* in social networks and similar communication mediums.

The Privacy of home concept addresses the physical resident of individuals. This is associated with ones' solitude and private affair that are well established in common law. This type of privacy concern can infiltrate to individuals' digital interactions when their information is spread across various sectors in machine.

Privacy in computing technology refers to the evolving relationship between the existing information and the information ownership by storing, processing, and distributing information [79]. Privacy concerns exist wherever uniquely identifiable data relating to a person or persons are collected and stored. In many cases these concerns refer to how data are collected, stored, and associated.

## 2.2 Privacy Protection in Information Management

Privacy introduced as: "the freedom from surveillances", "the protection of one's reputation", "protecting one from searches and interrogation", and "not selling one's information" [24], Privacy has been viewed from multiple perspective. Other researchers considered privacy interims: the limited access to self [28], the right to be alone [66]. Other views, based on "secrecy" [61] in which in many legal communities were accepted as definition for privacy. "control over personal information" [11], Intimacy and Personhood [65]. Privacy also viewed as "the condition of being protected from unwanted access by others" [65]. In [18] they define the privacy in context of the right to determine "to what extent information about people or companies is communicated to others".

In Cooperative Distributed Systems (CDS) perspectives privacy can be viewed in the context of *"information management"* [71]. The information in CDS environments the entities are autonomous, and they are able to interact and share information in behave of the information owner, in which this information can be processed or disseminated. Considering the setting of the entities in CDS, which are autonomists and self-interestedness, and autonomy of the entities in CDS settings, that might result a privacy concern.

The information management can be categorized based on the operations or the actions applied to the information including:

- Information Collection: Applying operations for gathering information from multiple sources such as the online (profiling, banking, tracking), collection of task specification and requirement.

- Information Processing: Applying operations for manipulating information such as aggregation, integration and identification.

- Information Dissemination: Applying operations for distributing information to multiple entities.

## 2.2.1 Personal Identifiable Information (PII)

Information or attributes such as SIN numbers and personal number can be used to identify entities. Some attributes can be used in combination of others to identify an entity; for example, combination of date of birth, gender, name and zip code. The attributes that directly identify the entities are called "identified" and the attributes that can [implicitly] result in identifying an entity are called "Personally Identifiable Information" (PII). In this context, attribute *disclosure* happens when the value of identifiable information reveals the identity of the entity. And, identity *disclosure* happens when the identifiable information is a bridge to associate sensitive attributes to an entity [43]. The challenge is that due to advances in technology and information processing which can convert the non-PII attributes to PII attributes at higher scale, it becomes not possible to directly identify PII [59].

Entities' incomplete knowledge in open environments originates the concern on the operations that might be applied on *shared* information. Combining information by applying operations to extract new information is known as a *secondary use problem*. This could lead to privacy concerns when the retrieved information is sensitive, and the information includes the identifier to the owner of the sensitive information. This issue which is functionally equivalent to the PII problem is due to *implicitly* extracting information from identifiable information that is *shared* [44],[70]. Resolving the PII problem has been investigated in three approaches; reduction, expansion and PII2.0. Reduction focuses more on "identified" attributes. For example, COPPA (Children Online Privacy Protection Act) concerns only with information about "identified person". In fact, the "identifiable" concept has been reduced from this approach. In the Expansion approach, the identifiable information is considered as critical as identified information. However, as almost any kind of information can be attributed to an identified entity, and from the practicality point of view, this approach is considered as a flaw. This is the result of treating the identified and identifiable information equally [44].

PII 2.0 is an approach for privacy in interactions that deals with PII problem through the perspective of risk analysis. Although, there are large amount of identifiable information, that could implicitly retrieve new identified information, not all of them have a high risk of privacy concerns. PII 2.0 introduces the risk of revealing information as a relative probability measure. If the risk of a set of identifiable information is high, then information should not be *shared* [44]. The risk of interaction is probabilistic view of the occurrence of associated negative impact of privacy concerns on the entity. It allows decision-making processes to evaluate the interaction and the sharing information with regards to the risk of interaction, gain and the possible drawback that might affect the entity.

In new forms of resolutions for PII complications, there are rule-based and standard-based approaches. Typically, the rule-based approaches are convenient when the area of social and technological development have reached a fairly stable state [57][1]. Due to the dynamic and open nature of environments in CDS, the rule-based solutions to resolve PII are not adequate approaches as privacy protection in distributed systems.

Privacy concern become a critical aspect during the era of the distributed systems, where the setting of its' environment is decentralized. The Distributed Systems can be categorized in more granularity classification that in this work address some of this classification that related to privacy models.

## 2.3 Privacy in Distributed Systems

Within the arena of distributed systems, privacy is a concern when the setting of the environment is decentralized. Distributed Systems can be classified in more granular categories that we address a few of them and discussed the related privacy models.

### 2.3.1 Privacy and Security in Authorization Framework

Most of the time Privacy and security have been similarly treated and interchangeable used. In which, the privacy has been misunderstood and be treated in the context of access control of entity. Frequently, the privacy has investigated, in the scoop of the information management, at the security authorization mechanisms [18][69]. Despite security mechanisms that are targeted to maintaining confidentiality, integrity and availability of the communication among entities, privacy concerns are about manipulating the information that could have been securely communicated [*shared*]. The efforts within security mechanisms are geared towards assuring the information is to be only accessible by the desired entity, and the entities' communication is not compromised with a third party. However, security mechanisms may not address the manipulation of information among entities. For instance, the communication with a search engine can have the required security measures and the integrity of the communication is supported. Nonetheless, the information that is retrieved by the search engine after applying operations on the collected information is not treated in security mechanisms. This indicates that the nature of security mechanisms is not sufficient to resolve privacy concerns. Privacy concerns are categorized on the control over *"how"* information is collected, processed and disseminated. Typically, the security mechanisms are applied on the established connection between at least two entities. If the confidentiality, integrity and availability of the communicated information are satisfied, that interaction is secured. Nevertheless, that does not guarantee that there is not privacy concerns with the interaction.

Diverse set of models has been applied on authorization in CDS such as SAML, Akenti, PERMIS, Shibboleth, VOMS, XACML, GT4 [18] and [69]. The objective of these models is to provide authorization platforms that protect information from unauthorized access. However, these models are still incapable of addressing privacy in relation with *"how"* information is processed and "*flow"* within entities. Additionally, the solutions do not provide privacy protection techniques for the collection and the dissemination of information. The work in [69] addresses privacy as part of the populated rules for the authorization mechanism. However, the model does not capture the identifiable information that implicitly can lead to privacy concerns. In addition, the setting of the applied model in this mechanism is assumed to include trusted entities to govern the privacy rules. Such setting is not necessarily attainable in all CDS environments and the privacy model cannot be applied.

### 2.3.2 Privacy Protection in Multiple Data Sources

Data source providers provide aggregated view of the information that is collected from people, business, and organizations. Typically, this information is published for research collaboration purposes and data analysis for a particular problem. However, the process of information collection can be pursued if exclusively, the aggregated information is published. *Disclosing* information such as the participation of an entity in the information collection process can lead to privacy concern for the entity. Many public data sources contain information that might be common across multiple data sources. Linking the available information across multiple data sources is based on their common information can identify individuals and *disclose sensitive information* which can be captured as identity *disclosure* and attribute *disclosure* [47],[27],[8]. These concepts depend on contextual variables, amount of released data, level of the knowledge of adversary [48], [57]. Given this categorization, there are different privacy models that address specific aspects of privacy. Models such as K-Anonymity [16], l-Diversity [8], SIPPA [57], t-closeness [34] and Differential Privacy [27] aim to resolve identity or attribute *disclosure*. The typical setting of anonymization mechanisms includes a trusted information collector that collects the information and disseminates aggregated information to other entities [20],[27][20],[34]. There are assumptions in this setting that the information collector is a trusted party and the process of information collection and dissemination happens in non-continuous fashion [38]. These mechanisms are tailored towards protecting sensitive information such as participation of entities in information collecting process. The adversary consumes the aggregated information in conjunction with previous knowledge to retrieve sensitive information about an entity. Evidently, not all CDS applications can adhere to the setting of anonymization mechanism. Furthermore, because of possibilities of attacks such as complementary attack in K-Anonymity [47], these approaches are not applicable in CDS. In complementary attack, the adversary accesses the published anonymized information in multiple sources and combines them all. This in many cases circumvents the protection that is applied.

### 2.3.3Privacy in Distributed Constraint Satisfaction

Distributed Constraint Satisfaction Problem (DisCSP) is a Constraint Satisfaction Problem (CSP) in which the variables and constraints are distributed among distributed multiple entities (i.e., Agents). Those agents need to determine values for a set of variables such that the cost of a set of constraints over the variables is satisfied and thus optimized (as either minimized or maximized). In other words, CSP is about finding a consistent assignment of values to variables [43][52]. The DisCSP framework was a focal point of several areas such as Artificial Intelligent and agent Technology. In DisCSP, privacy principles have been identified at four level [8] namely: 1) The Agent, 2) The Topology, 3) The Constraint and 4) The Decision. At the Agent level, the algorithm has to guarantee that no agent can learn the identity of any other agent unless they are in sharing coordination constraints. At the topology level the algorithm should not allow any agent to learn about the constraints and cycles of other agents. For example, the constraint of an agent for specific resource is sensitive information that should be kept private. The Constraint level is similar to topology level with focus on constraint and its relations. Finally, at the decision level, the algorithm has to protect the outcome of any decision that the agent makes. The solution in [15] expands the Distributed Pseudotree Optimization Procedure (DPOP) algorithm [6] by adding privacy metrics. This algorithm creates a Depth First Search Tree (DFS tree) out of entities. Each entity interacts only with their neighbors. Entities send their constraint to their parent, and the root node (leader) accordingly solves the problem and sends it back to others. The contribution of the solution in [15] anonymizes the construction of DFS. Nodes have code names for interactions. Moreover, the leader in each round is anonymous and given the associated assumptions, the approach can guarantee the required privacy levels. However, the settings in these environments are limited to the topology that is defined in priori and the maximum distance between two nodes in the environment which is known for the used algorithm. Evidently, the adoption of the solutions in DisCSP in CDS will not inherent to all settings of application. Furthermore, in this algorithm, it is possible for a malicious entity to forge the coordination information in attempt to be the leader which may perform actions that can cause privacy concern.

In addition, there are attempts to resolve privacy concerns in DCOP (Distributed Constraint Optimization Problem) [63][64]. DCOP consists of entities that set and control the evaluation of variables. Entities decide which evaluation of the variables has more benefit for them. However, the problem’s setting is based on the assumption that all entities are aware of the constraints of other entities, and only the evaluation of the variables is sensitive information [64]. Additionally, privacy solutions in DCOP are derived from an information theoretic perspective [64] and do not necessarily reflect on the privacy concern in setting in CDS environment.

## 2.4 Privacy in Distributed Artificial Intelligence

Multi Agent System (MAS) is one of the computational models applied in CDS in which the computational entities operate in a decentralized control fashion and modeled as autonomous entities known as agents. MASs are designed for autonomous actions and flexible interaction [14] where it addresses autonomy by drawing on concepts and techniques from artificial intelligence. Agents act on behalf their principals and engage in various interactions that might require in many cases the exchange of personal information [39]. This, as such makes privacy management an essential aspect.

Privacy management approaches in MASs has been categorized into three categories: (i) policy-based, (ii) privacy utility tradeoff and (iii) social relationships. For instance, the work in [34] is a policy-based framework in which a trusted broker compares the policies of providers and consumers and decides on their compatibility. The broker resumes any interaction only if the compared policies are compatible. However, the approach relies on the assumption that the broker is a trusted entity [39]. The Privacy Enhancement Agent (PEA) [33] is a similar approach that uses P3P (Platform for Privacy Protection)[51] retrieve the P3P policies, validate the compatibility of policies and accordingly decide on the possibility of further engagement in any interaction.

Other approaches adopt the ontological comparison of policies that are described and represented using the Web Ontology Language (OWL) [67]. Once the conditions are accepted among both parties, the consumer *shares* the information. In similar approaches, the rules are semantically analyzed, and the access control mechanism are incorporated with the privacy rules [6][37]. However, in these models, there is a lack of mechanisms which obliged entities to comply with the commitments [[39].

One of the major challenges in privacy management is to identify and measure the *risk* of *sharing* the information. To deal with such issue, “Privacy- Utility Tradeoff”’ mechanisms were proposed [7][39]. This work is based on calculating the information gain of *shared* information. The elements such as history of two sides of interaction, social aspects of interaction, relevancy of requested information to the offered service has not been considered in these mechanisms. This motivated the complementary approaches that applying concepts of trust and intimacy in measuring risk and utility. The challenge with these approaches is the difficulty of validating these metrics, in particular in CDS environments [39]. The utility trade off mechanisms evolved with approach of measuring the risk of privacy concerns. The risk of interaction adheres to execution of operations that might cause privacy concern, but it can measure the probability of the entity’s data getting used [9].

## 2.5 Privacy Protection in Cooperative Distributed Systems

Many solutions are proposed for computations for which the environment is modeled as CDS. Typically, the prospects of these models are tailored towards particular setting of the environment where a certain type of information is exchanged in the interaction of entities. Adopting these solutions for many applications of CDS imposes limitations and assumption of their environments. In the following we address some of the related works within this area.

### 2.5.1 Privacy in Auction Mechanisms

Auctions are subclass of markets that restrict the governing rules of the market in which buyers and seller are trading goods and services. Auction mechanism design is the attempt to manipulate the rules of the auction in order to achieve specific goals [40]. In auction configurations, an auctioneer applies the rules of the auction mechanism and rewards the winner(s). In this setting, it is possible that a faulty or malicious auctioneer forges the auction or exploits the bidding values [52]. When bidders submit their bids to the auctioneer, it is possible that the auctioneer exploits the bidding value of the winner for the future auctions. For example, if the winner’s bid is $900 and the second bid value is $600, then the auctioneer can start the auction from $900 since it has the knowledge that at least one entity will bid with this value [52]. It is very desirable and an important aspect of bidding activities to assure the bidders about the safety of the auction with respect to privacy concerns.

To deal with this issue some approaches were proposed in the literature [43] [52]. The work in [52] an Auction Issuer (AI) is introduced which is a passive entity that has no direct communication with bidders and limits the auctioneer ability to only access the relevant information. The AI in this architecture computes the auction and presents it back to the auctioneer. This restricts the auctioneer to be able only to know the identity of the winners only and not the value of the bids. However, this protocol cannot guarantee the privacy of entities when collusion takes place between the AI and auctioneer. The (AI) entity is designed to control the access of auctioneer entity to sensitive information.

### 2.5.2 Risk Analysis

Risk analysis in interactions of entities has played a significant role in many privacy solutions. Identifying risk levels in a system provides meaningful measures which can be applied to processes that could mitigate the risk [36]. Risk in general is a degree of belief on occurrence of an event with undesired outcomes. The risk of interaction refers to level of belief on incidents and events in which *sharing* information in interaction led to privacy concerns. There are various models to capture the risk of interactions. Some of them adhere to analyzing the interactions in terms of 1) Information Sensitivity, 2) Information Receiver, 3) Information Usage [67] Other approaches use fuzzy logic to capture the effecting variables on risk of interactions. The work in [4] utilizes hierarchical fuzzy inference system to address the risk of interaction. It measures and evaluates the relevancy of the requested information; trust level, cost and criticality of the shared information, type of intended operation, the content of the agreement, sensitivity of information and information gain in a given interaction. Using these variables, a hierarchical fuzzy system can be developed to measure the risk of interaction.

### 2.5.3 Targeting Advertisement

Targeting advertisement systems apply Online Behavioral Advertisement (OBA) techniques to promote more relevant commercial contents to users. Because of capability interdependency among entities of these systems, they need to exchange information such as user's interest that might be sensitive. In this context, privacy becomes a major challenge [76][65]. One of the approaches in addressing privacy concerns is through Adnostic [76] In Adnostic system, privacy is modeled as a tuple that is expressed in terms of the following attributes <consumer's identity, consumer's request>. The disclosure of any relevant attribute may result in privacy concern to consumers. In this system, it was presumed that, providers are able of delivering their capability without knowing the identity of consumers. The objective of the model is to protect consumer's privacy by introducing a trusted entity called Trusted Third Party, (TTP). Providers and consumers are defined as roles, which can be played interchangeably. A provider has to present a list of options to the consumer whose in turn consumer selects the preferred information which will be considered as the request information. However, consumers encrypt the list of options including the one that was tagged as the chosen option. When providers receive the encrypted list, they only know that an item is selected but they are now aware which one is chosen [76]. In Adnostic, it is assumed that there is a time period where providers have to wait before providing their capabilities. In this time, they need to collect all encrypted lists of options sent by consumers, aggregate all these lists and submit them back to the TTP at the end of waiting period. The TTP is capable of decrypting the list and thus delivers the decrypted list to the provider. The provider's access to an aggregated list of requests does not show which identity has chosen which item in the list. Another approach in targeting advertisement is through decoupling the request and identity utilizing ElGamal crypto systems [2]. However, in these approaches, the protection mechanism can be circumvented if entities collide [44]. Furthermore, the only sensitive information in this model is the combination of consumer’s identity and their requests. This makes the system incapable of managing various settings in CDS environments.

### 2.5.4 Privacy Protection Management in CDS

In the message-based form of interactions, entities exchange information through autonomous and self-interested entities, and thus their privacy becomes a concern. In CDS, solutions are accomplished through the participation of several entities where each has only part of the solution. In [56] a generic brokering has been introduced, where the brokering architecture has been defined to enable cooperation under a desired level of privacy protection in CDS. For which, an agent-based brokering framework that provides seamlessly coordination solutions and presents additional privacy opportunities to various participants within cooperative distributed systems has introduced. Where the privacy protection has been treated as a design issue in developing brokering services for cooperative distributed systems. In such a setting the privacy mainly driven by the broker, in such setting the broker is an entity that is able to process, aggregate and disseminate information. However, the approach relies on the assumption that the broker is a trusted entity [39][56]. This work will not be applicable to be applied since the broker entity is exposed to all of the entities information, and that make it unacceptable if the broker entity compromised by and adversary or the information has been aggregate the shared information for future purpose that can breach the privacy of the information owner. Where in the work [71] consider the privacy protection as a computational aspect. In which, the privacy protection management framework at the interaction level as a computation element by expanding the structure of the entity to include privacy protection management that convert the entity to be a privacy aware entity. Applying the privacy protection management framework will capture the privacy concerns at the interaction level. Since the interaction is governed by the interaction protocol, the framework captured even the privacy concerns that can be yield through the interaction operations. It is proven in this work that protection at the interaction protocol is sufficient for protecting privacy in CDS environments. Also, the generated privacy-based interaction protocol has quantifiable privacy protection level that allows entities to interact with a certain degree of protection [71].

## 2.6 Summary

In [71] formally explained that legitimate acceptable solutions at the computation that require the inclusion of privacy resolution in-addition to problem solving and coordination has been introduced. However, the work was a definition to the privacy protection of a privacy concern and a computation solution has been proposed with a privacy protection-based interaction protocol utilizing the proposed framework and extending it with the practically aspect in the context of open environment, in which the proposed framework will be sufficiently adequate for the open environment.

Despite the variety of works carried out toward protecting privacy in different disciplines, an adequate practical privacy model for CDS environment is lacking. Within the context of information management, privacy can be categorized as information collection, information processing, information dissemination and invasion. One of the challenges of the privacy concept is the identification, which is referred to manipulating information in order to retrieve and relate “sensitive information” to entities. However, information may have different risks for the identification. Identified information can directly lead to the risk of inferring and identifying an entity. The setting of these two categories is different, which makes it not possible to differentiate among them.

# Chapter 3

# 3 Privacy Concerns in CDS: Concepts and Models

Privacy is an area of research that includes a variety of applied models that are automated in different applications. Some applied models require settings that impose limitations on the design of entities in the environment and subsequently create a *closed* environment. This requires employing models that can capture privacy as a computational concept which necessitates a formal analysis of privacy. Privacy in an information management context enables modeling in a computation context where the flow of sensitive information becomes a privacy concern. This chapter includes a formal analysis of privacy and modeling in the context of information management.

## 3.1 CDS: An Agent-based Model

CDS is a class of systems in which entities are autonomous, self-interested, able to operate on some functions locally, and exercise some authority in sharing their capabilities. Goals in these settings refer to a state in which the actions of the entity - including physical and mental reasoning. Within CDS, entities have interdependencies through which some goals may be unattainable through the abilities of an individual entity.  They may require coordinating activities with other entities to reach an individual or collective goal state [32][56][71]. This coordination is a class of solutions that provides structure and mechanisms to the system to address interdependency issues. “Structure” refers to the entities’ pattern of communication and decision-making related to coordination. “Mechanisms” are a composition of decision points, coordinated control and interaction devices directed to resolve problems with interdependencies [32]. An essential characteristic of CDS is the distribution of control which prevents outside parties from controlling the strategies of entities. This supports the concept that every entity in CDS is part of the solution in which participating entities’ goals are achieved.

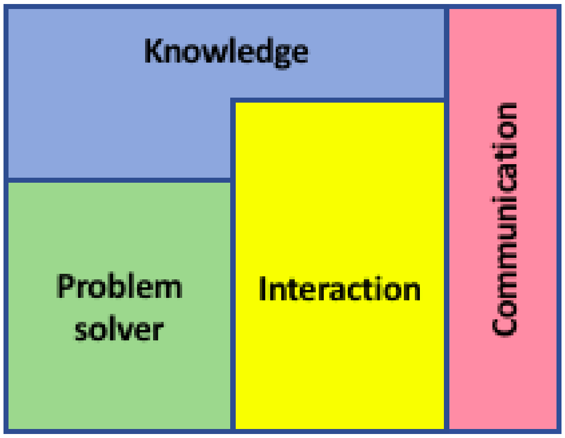


**Figure 2: Computation Entity in CDS**

This dissertation focuses on entities of CDS in an agent-based model. Entities can be modeled as CIR agents Figure 2. These agents are organized by knowledge, problem solving, interaction, and communication capabilities [32]. “Knowledge” is the entity’s mental state about the world, a concept often missed in examples of CDS environments. In these examples, global knowledge is distributed among all entities. “Problem solving” refers to the entity’s ability to identify the class of their goals, categorizing sub-goals, applying required actions to the goals’ state, and determining the type of interdependency. “Interaction” is the authority and capability of the entity in the pursuit of mechanisms that can resolve interdependency problems. Interaction mechanisms are steered by protocols that manage engagement between entities. The “communication” layer is responsible for packaging and transferring messages in the desired languages. [32] Communication-based interaction, or message-based interaction, is essential when the entities’ knowledge is incomplete, and they are obligated to exchange messages. There are interdependency issues with settings in CDS, and as such reaching a solution requires the interaction of multiple autonomous entities. This indicates that computation in CDS takes place within interactions among entities.

In the open structure of CDS environments, entities’ availability and participation is unpredictable and there is therefore no control over their behavior or the design they adopt.

New forms of computation emerging in Grid, cloud, and mobile computing can be modeled as open CDS. Cloud paradigms such as IaaS, PaaS, and SaaS are used in many application domains medical, health, financial, entertainment, education, business, and communication.

## 3.2 Privacy Concern Analysis and Model

Privacy concerns occur in environments with multiple autonomous entities. This is a natural characteristic of the environments where autonomous entities exchange information. Let $E$, be the decentralized environment of autonomous self-interested entities $e_N$

$$E = \{e_1, \dots, e_N\}$$

In the context of information management, entity $e_i$ can be modeled in terms of information $I_i$ and operations $O_i$. At the lowest granularity level, an entity can be shown as:

$$e_i = < O_i, I_i >, 1 \leq i \leq N\ i.$$

Where

$$I_i = \{I_{i,1}, \dots, I_{i,t}, \dots, I_{i,N}\}$$

$$1\ \leq t \leq N$$

and

$$O_i = \{O_{i,1}, \dots, O_{i,t}, \dots, O_{i,N}\}.$$

Entities have various states [24]. Information about an entity can be viewed as the state of an entity. In many cases, an entity desires to protect a certain state from being exposed to the outside environment; or to protect part of the information being exposed to a specific part of the environment. This information can be referred to as *"sensitive information"*.

The flow of sensitive information can vary within a context of a group of entities in the environment. Family is an example of a group in society in which individuals have distinctive approaches to how information flows between participant entities and outside the group. As a result, for any given state of an entity, there is a boundary for exposure $E_{i,k}$. This suggests that privacy is the state of exposure boundary of an entity's state with the outside environment $E$. There exists an exposure boundary for any information, including those entities that are considered to be inside the boundary

$$E_{i,k} = \{e_{i,1}, \dots, e_{i,t}, \dots e_{i,N}\}, (E_{i,k} \subset E), 1 \leq t \leq N$$

Information $I_{i,k}$ might be "*Sensitive*" $I^S$ in relation with a particular entity $e_j$ and non-sensitive to others. When the information remains within the exposure boundary it is considered non-sensitive; however, once information flows outside the boundary it is considered sensitive. For example, salary information is not sensitive within members of a family, but it may be sensitive for those outside the family. The exposure boundary is designated by the information owner entity $e_i$. Therefore, sensitive information is a relative classification between the entity that possess the information and the others who exist in the environment.

$$I^S(I_{i,k}, e_j) = \ (e_j \notin E_{i,k})$$

As previously noted, based on an entity's interaction, information can be classified as sensitive or non-sensitive in relation with the entity interacting with. Also, information can also be classified as implicit in relation to operations that can be applied on the explicit information. Implicit information can be transformed to explicit information by the execution of an operation. This means that an operation can be modeled as a function that extracts implicit information from explicit information. An operation can also combine the explicit information with other shared information (denoted as $I^{sh}$) to transform the implicit $I^{im}$ information to explicit $I^{ex}$. The shared information $I^{sh}$ is collected or inferred information, which it does not reflect the privacy of any information on its own. $I^{sh}$ can expose information about an entity if used in combination with other $I^{ex}$ information. Therefore, any implicit information is equivalent to some explicit information that can be defined as follows:

$$o(I^{ex}, I^{sh}) = I^{im}$$

Manipulation of explicit information by applying operations can transform implicit information into explicit form.

$$\bar{\bar{o}}\left(I^{ex}, I^{sh}, I^{im}\right)$$

Illustrates that Executing Operation (o) on explicit information $I^{ex}$ transforms the implicit information to an explicit form of $I^{im}$. In contrast,

$$\bar{\bar{o}}\left(\widetilde{I^{\imath m}, I^{ex}}\right)$$

is used to show the execution of an operation that is prevented or neutralized. And in this case, the application of the operation cannot proceed.

The flow of the information $I_{i,k}$ that belong to the entity $e_i$ with a particular participant entity $e_j$, is not considered to be sensitive $\neg I^s$ . As such, "sharing" is defined as a process that takes place only within the exposure boundary and can be formally expressed as:

$$S\left(I_{i,k}, e_j\right) = \neg I^s\left(I_{i,k}, e_j\right)$$

Through "sharing" non-sensitive explicit information, it is possible to *disclose* implicit information by introducing an operation $o_{j,w}$ on the shared information $I_{i,k}$. This might result transforming non-sensitive information $\neg I^s$ to sensitive information $I^s$. The implicit information can be labeled as sensitive or non-sensitive. This suggests that the *disclosure* of information can result in transferring information outside of its exposure boundary.

For instance, Ali’s mark in a specific subject is classified as sensitive information. For example, Ali shares with Amy information, which states that his mark is 10% percent more than the average mark of his colleagues. If Amy has an operation that is capable of retrieving the overall students’ average mark, she will be able to extract Ali’s mark. In this example, the statement “Ali’s mark is 10% percent above the average of all the student marks is explicit information, while Amy’s operations and this information implicitly refer to Ali’s mark which is considered being sensitive. This illustrates how implicit information may convey sensitive information and by transform it into explicit information will reveal the implicit sensitive information.

$$D\left(I_{i,k}, e_j\right) = o_j\left(I_{i,k}\right)$$

Although entities have the authority to protect their relevant explicit sensitive information by not *sharing* it outside the boundary, there are concerns when the implicit information is transformed into explicit sensitive information.

Given the earlier example, $I_{Ali,k}$ is representing the statement “Ali’s mark is 10% percent less than the average mark of his classmates”. Amy also belongs to the exposure boundary $E_{Ali,k}$ where implies $\neg I^S(I_{Ali,k'}, e_{Amy})$. If Amy has a retrieval operation $\left(o_{Ali,ret}\right)$ on a statistical dataset that includes the students average marks $I^{aux}$ and calculates Ali’s mark, $o_{Ali,ret}\left(I_{Ali,k'}, I^{aux}\right)$ is the implicit information that reflects Ali’s mark $\left(I_{Ali,k'}\right)$.

$$\bar{\bar{o}}_{Ali,ret}\left(I_{Ali,k}, I^{aux}, I_{Ali,k'}\right)$$

This suggests that if Amy executes $\bar{\bar{o}}_{Ali,ret}\left(I^{aux}, I_{Ali,k'}\right)$, she can extract Ali’s mark. Disseminating information ultimately can be modeled by operations where the functionality of the operation is to transfer the information to other entities. As an example, Amy may perform an operation to send $I_{Ali,k}$ to Shawn.

One of the main challenges of privacy relates to the execution of operations that convert sensitive implicit information to explicit form. As such, having knowledge about the operations of the entity that receives the information can indicate what sensitive information can be retrieved. This introduces the concept of authorized operations. $O_j^{i,k}$ is a set of operations belonging to $O_j$ where $e_i$ has agreed to their application on $I_{i,k}$. In this case, the privacy concern is related to applying operations that transform explicit information to the sensitive form of this information. This leads to privacy concerns about sensitive information as a result of transferring information outside the boundary through non-authorized operations.

Modeling privacy as a computational concept requires identifying measures that can reflect privacy in a computational model. The concepts that explain the state of privacy among interacting entities are applied in managing measures that can be associated to computational concepts.

When entities share information, they agree on the terms of utilization of the shared information. These terms can be enforced through the norms of various cultures in people societies [22] or electronic legal agreements among web services [78] Ideally, these agreements include a permitted set of operations that can be applied on the shared information. Not disobeying the established agreement through the execution of non-authorized operations $O_j^{i,k}$ is considered evidence of a privacy violation. For instance, in the above example, if $e_j$ executes a non-authorized operation $o$, then it is said that $e_j$ has violated the privacy of $e_i$. Accordingly:

$$-\left(\hat{O}_j^{i,k}, O_i, O_j^{i,k}\right)$$

Where:

$$\hat{O}_j^{i,k} = \left\{\hat{O}_{j,1}^{i,k}, \dots, \hat{O}_{j,t}^{i,k}, \dots, \hat{O}_{j,T}^{i,k}\right\}, 1 < t < T$$

The non-authorized operations can also be defined in relation to all of information about an entity.

$$\hat{O}_j^i = \bigcup_{k=1}^{M} \left(\emptyset, \hat{O}_j^{i,k}\right)\ 1 < k < M$$

Based on the scope of communicated information through *sharing* and *disclosure*, non-authorized operations can also be applied $\hat{O}_j^i$ on a subset of information $(S)$.

$$\hat{O}_j^i(S) = \bigcup_{\forall s\left(s \in PS(S)\right)} \left(\emptyset, \hat{O}_j^s\right)$$

A computation system $(C)$ including entities $(e)$ provides a solution $(S)$ to a problem $P$ by applying computation processes $Cp$ [71].

$$C\colon e \times P \times CP \to S$$

*DEFINITION 1:* $(S)$ *is an acceptable solution* $\left(s - accept(s)\right)$ *as it resolves the problem and does not result in privacy concerns* [71].

*DEFINITION 2:* Privacy Model in the context of sensitive information $(P - Model)$ [71] is:

$$P\colon \left\{e_i, e_j\right\} \times I_i \times O_j \to \bigcup_{k=1}^{k \leq M} \neg I^s(I_{i,k}\ , e_j)$$

## 3.3 Privacy Concerns Management

Due to the fact that computation in CDS takes place at an interaction level where entities exchange information, then modeling the privacy protection in the context of the information management is reasonable for CDS in open environment. Moreover, the message-based interactions in CDS can be modeled with information management into information collection, processing and dissemination. Modeling privacy in this manner enables application of the privacy protection model in interactions. Through which, privacy protection becomes part of the computation. The interactions are steered by interaction protocols that are abstracted as a set of messages and sequences. By incorporating the privacy model at the interaction level, it creates a privacy protection management framework. This expands interaction protocol messages and sequences that are supported by privacy protection mechanisms.

The concern of non-authorized characteristics of an operation that relates to the interacting entity. Entities agree on set of operations that cannot be executed over the shared information. This is considered to be the agreement $\theta_{i,j}^{i,k}$ between entities $e_j$ and $e_i$ by executing non-authorized operations $\hat{O}_{j,w}^{i,k}$ on $I_{i,k}$:

$$PV\left(e_j, I_{i,k}, \hat{O}_j^{i,k}, \theta_{i,j}^{i,k}\right) = \exists\, w \mid \theta_{i,j}^{i,k} \wedge \left[\bar{\bar{\hat{o}}}_{i,w}^{i,k}\left(I_{i,k}\right)\right]$$

While the privacy violation $(PV)$ is about disobeying the agreement among entities, while privacy protection is about enforcing mechanisms that prevent application of non-authorized operations on entities' information. Hence, the privacy protection $(PP)$ is about preventing execution of non-authorized operations on all subsets of information.

$$PP\left(e_j, \left(PS(I_i)\right), \hat{O}_j\right) = \forall t, w \mid \left(t \subset PS(I_i)\right) \wedge \bar{\bar{\hat{o}}}\widetilde{_{j,w}^{t}\ (t)}$$

Preventing the processing of $I_i$ using the operation o is considered privacy protection. Operations in this type of protection mechanisms requires an awareness of what operation will be applied on information. If non-authorized there will be no result or if authorized, the result will be provided.

The punishing approach in privacy protection mechanism is applied in situations where preventing *sharing* information is not possible. However, some operations provide assurances to owners of information. If a collecting entity violates privacy requirements, the owner of the information may execute punishing operations. An example of this approach is terms and conditions that are accepted by both entities. If any operation outside of the agreement occurs, there are legal consequences for the non-compliant entity.

When preventive mechanisms cannot be applied, the punishing mechanism is an option. For instance, when a service provider interacts with a consumer in a different time period, the information that is aggregated in this period can be used to transform sensitive implicit information to explicit using auxiliary information. In this case, punishing mechanism are more effective. Such punishing mechanisms support agreements between two entities which enforce the execution of consecutive action towards the faulty entity.

Protection mechanisms can be applied at information and operation levels. Typically, protection mechanisms at the information level limit the access of entities to the information that is shared. As an example, sensitive information accessed through adequate resolving of a requested task is nonetheless not disclosed. Still, this may be inadequate in relation to applications that require receiving the non-distorted complete information. To address this, protection mechanisms at the operation level are more advantageous.

## 3.4 Privacy Protection in CDS

The analysis within this research indicates that among existing privacy models, attending to settings can be inadequate for CDS environments. The privacy model in CDS has to be captured at computation and therefore requires a formal modeling of privacy. The proposed formal privacy model is in the context of information management where entities are modeled as a set of information and operations. Information management is categorized as information collection, processing and dissemination [71].

CDS is a class of systems that is positioned as a computation platform in which computation occurs based on the interactions of entities. Solutions in CDS are achieved by participation of entities in a distributed decentralized fashion. This requires resolving the interdependency problem through coordinating activities that adopt interaction mechanisms.

In the incomplete knowledge environment, entities update their knowledge about the environment and solve their problems through message-based interactions.

*THEOREM 1:* Any incomplete knowledge CDS computation is an$(i - mng)$ [71].

The computation $C$ in incomplete knowledge CDS toward a solution $S$ happens in interactions $In$ among entities $E$ therefore:

$$C: E \times In \rightarrow S$$

Due to the assumption that entities have incomplete knowledge in CDS, knowledge in modeled as information; and interaction is modeled as information collection, processing and dissemination which can be abstracted as operation and information. Hence:

$$In =< I, O >$$

$$C: E \times In \rightarrow S$$

$$C: E \times I, O \rightarrow S$$

Giving *DEFINITION 1and DEFINITION 2* and based on *THEOREM 1* computation in incomplete knowledge CDS can be modeled as information management computation.

*THEOREM 2:* Let $(P)$ be a $(P - Model)$. For any $(i - mng)$, $(P)$ *is essential to have* $(s - accept)$ [71].

$$(P - Model): \{e_i, e_j\} \times I_i \times O_j \rightarrow \bigcup_{k=1}^{k \leq M} \neg I^s(I_{i,k}, e_j)$$

$$C: E \times I \times O$$

$$\forall i, j, k \mid Q = \bigcup_{k=1}^{k \leq M} \neg I^{s}(I_{i,k}, e_j)$$

$$if \ \exists \ s, \in (s, S) \mid \ \notin (s, Q) \rightarrow \ \neg\big(s - accept(s)\big)$$

This affirm that the acceptable solution must include the $(P - Model)$.

Therefore, computation in incomplete knowledge CDS can be modeled as information management computation, which based on *THEOREM 2* affirms the proposed privacy model is applicable and required to achieve acceptable solutions.

### 3.4.1 Privacy Protection Mechanism

Managing privacy protection requires a protection mechanism, where the privacy protection mechanisms require knowing the operations of entities and being aware of what operations are authorized. In various instances in CDS environments, the assumption is that the knowledge of entities is incomplete which implies uncertainty about the entities and their operations. Capturing this uncertainty provides levels of knowledge about the operations which affirms the exercise of quasi-protection mechanisms in varied CDS environments.

Quasi-protection mechanisms convey levels of uncertainty about the extent of non-authorized operations that the mechanism can prevent from execution. For instance, anonymization techniques can provide privacy protection with a degree of probability [20], [27][23]. Others, such as rule-based mechanisms for protecting privacy, are capable of supporting a limited number of non-authorized operations [18][69]. The uncertainty level in these cases is captured as Privacy Protection Level (PPL). PPL is a probabilistic base model to describe the effectiveness of a mechanism to prevent or neutralize non-authorized operations from producing sensitive information. This measure can be associated to computational concepts. The execution of the mechanism $\mu$ in relation to protecting privacy $(PP)$ is the space $S$, in a way protection mechanism can prevent the execution of a non-authorized operation:

$$\bar{\bar{\mu}} = PP\left(e_j, S, \hat{O}_j^i(S)\right)$$

By applying the mechanism over the space of entities' information set, there is a level of uncertainty associated with the application of the protection mechanism which implies the conditional probability protecting privacy by executing $\mu$ given the space of $I_i$. In another word, the probability of $\mu$ protecting privacy is measured when it is applied on $I_i$.

$$PP\left(e_j, I_i, \mu\right) = P(\bar{\bar{\mu}}|I_i)$$

This can be measured either statistically or characteristically. For instance, in a simplified view, in a complete knowledge world where entities have the knowledge over all communicated information, in a discrete set of operations and an algebraic form, evaluating PPL depends on non-authorized operations that are prevented from application by applying the mechanism $(z)$ to all non-authorized operations $(n)$; $PPL = \frac{z}{n}$.

PPL is a measure that predicts privacy protection in an interaction among two entities. Depending on the context and architecture of the environment, PPL might be evaluated differently using the same approach. As an example, in this section, PPL is evaluated based on differential privacy [27][20]. A randomized function $(K)$ is $\in -differential\ privacy$ if for all databases $(D_1)$ and $(D_2)$ differing on at most one element and all $S \subseteq Rang\ (K)$.

$$\Pr[K(D_1) \in S] \leq \exp(\in) \times \Pr[K(D_2) \in S]$$

To achieve differential privacy, a mechanism is required that can implement differential privacy [71], [68]. The probability of a mechanism implementing differential privacy is $1 - 2 \in$.

Considering $(n)$ as number of non-authorized operations [queries] in info collector, implementing $\in -differential\, privacy$ in $(z)$ number of non-authorized operations has $(1-2\in)$ probability in each of them. Therefore, it creates a binomial distribution in which the expected value of $(z)$: $E(z)=n(1-2\in)$. This leads to $PPL=1-2\in$.

Differential privacy is a model for creating randomized function that has been applied in various statistical databases including anonymized datasets. Where it collects and share aggregate information about user habits, while maintaining the privacy of individual users participants share some information with an info collector which is sensitive to share with another entity.

$$S(I_{k,1}, e_i) \rightarrow \neg I^s(I_{k,1}, e_i)$$

$$\neg I^s(I_{k,1}, e_i) \rightarrow I^s(I_{k,1}, e_i)$$

There is some auxiliary information about participants that is possessed by the adversary. It can be explicitly received or implicitly inferred.

$$D(I_{k,\mathrm{p}}, e_j) \rightarrow (I_{k,\mathrm{p}} \in I_i)$$

The info collector applies a mechanism [differential privacy] to prevent the execution of $(o_{j,n})$. Differential privacy mechanism enables the info collector to include noise information to the result of each query. The outcome is new information that cannot be used for retrieving $(I_{k,1})$.

$$PP\colon o_{i,m'} \mid \bar{\bar{o}}_{i,m}, (\{I_{k,1}, D, DB, I_{i,b}\}) = I_{i,b'} \wedge \bar{\bar{\hat{o}}}_{j,n}^{k,p}(\{I_{k,p}, I_{i,b'}\})! = I_{k,1}$$

Utilizing the differentially private randomizing functions is motivated by modeling privacy protection at the participation of entities. In the other word, privacy protection is the state of producing outputs [explicit information] in which participation of any single entity does not impact the result to a large extend. This argues that "participation of an entity in a statistical database" is the information that privacy protection is targeting. This suggests that "participation" is considered to be sensitive information.

Sensitivity is in direct relation with the perception of an entity about the recipients of information [45]. However, the above analysis illustrates that there is an assumption in differential privacy which only considers the "ownership" of information as sensitive information. This is the reason that sensitivity is captured at the operation level. The result of all operations will be incorporated with the levels of noise which can satisfy the conditions of differentially private functions.

Privacy protection mechanisms are operations that are applied on information and provide the necessary information for privacy protection.  This indicates the structure of privacy protection mechanism is the set of operations it applies $(O^{\mu})$ and the set of information generated by the operations $(I^{\mu})$.

$$\mu = (O^{\mu}, I^{\mu})$$

Privacy protection mechanism can also be categorized as preventive and punishing. When mechanism operations are applied before *sharing* information, it is preventive and when it is practiced after non-authorized operations are executed, it becomes a punishing mechanism.

*DEFINITION 3:* A computation system including entities $(E)$ that provides a solution $(S)$ to a problem $(P)$ by applying computation processes $(CP)$ [71].

$$C: E \times P \times CP \rightarrow S$$

*DEFINITION* 4: $(C)$ is Information Management computation system $(i - mng)$ when problem and solution are modeled as information and computation as operation [71].

Operations in information management can be classified as collection, processing and dissemination that can be executed by entities $(E)$.

As it has mentioned *in DEFINITION 1:* $(S)$ is an acceptable solution $\left(s - accept(s)\right)$ as it resolves the problem and does not result in privacy concern.

# Chapter 4

# 4 Privacy Protection Management Framework

The assumption is that requester entities have various expectations and preferences with respect to privacy from potential provider entities, and that these expectations and preferences change in different contexts and at different times. In the proposed model, the risk of interaction of entities is a measure to determine proceeding interactions. If the risk of interaction is not acceptable to the requester entity, it will refuse and search for alternatives. Otherwise, entities take the risk and share the required information [58]. Under this assumption, the proposed framework can evaluate the risk of interaction and possible privacy protections to enable entities to make decisions that can protect their privacy and resolve the interdependency problem.

## 4.1 Privacy Protection at the Interaction Level

As noted in Chapter 3, CDS privacy protection can be reduced to operations and information which enable it to be part of information management. In which, in the context of information management, information can be categorized as information collection, information processing and information dissemination. Information management is deployed at the interaction level where the computation takes place and information is collected, disseminated or processed. Providing privacy protection at the interaction level is an architectural approach that can benefit various applications. In a way, the participant entities are utilizing interaction protocols to resolve their interdependency problem.

The initial point where the entities start sharing their information is during the interaction among the participant entities. The focus of this research is on message-based interactions. Providing the privacy protection mechanism at the interaction protocol enables applications to delegate the privacy resolution procedure to the interaction protocol, and the solution space of those applications will be limited to entities that can protect entities' privacy.

### 4.1.1 Privacy-Based Interaction Protocol

The interaction is modeled based on the type of the interdependency issue that the protocol is designed for, which is solved through the interaction.

$$Interaction\ = < \delta, e_i, e_j, IP >$$

$\delta$ is the type of interdependency [32], and $e_i$ is the entity that requires the capabilities of other entities, such as $e_j$, to solve its' capability interdependence issue. Interaction protocol $IP$, is acquired by the participant entities to coordinate their activities. Message-based $IP$ is modeled as a set of messages $M$ and the pattern of sequences $S(M)$ that includes messages that are exchanged among entities. Sequences in the $IP$ refer to the pattern of the exchanged messages. The given sequence indicates where information is collected and disseminated. As described in the proposed privacy model, collecting and disseminating information can be reduced at the operation level. Similarly, the existing sequences of an IP also can be modeled by the sequence of operations $o^{IP}$. Therefore, the structure of $IP$ can be reduced to operations and be modeled as:

$$IP = [o^{IP,1}, \dots, o^{IP,q}, \dots, o^{IP,Q}]$$

To protect privacy at the interaction level, privacy protection mechanisms should be incorporated into the operations of the interaction protocol. As discussed, privacy protection mechanisms have a set of operations $o^m$ that are executed in a specific order:

$$O^{\mu} = [o^{m,1}, \dots, o^{m,d}, \dots, o^{m,D}]$$

The assumption is that the privacy protection mechanism involves entities that match with the architecture of the interaction protocol. The privacy protection management framework requires transforming the interaction protocol to a protocol that is integrated with privacy protection mechanisms and delivers the solution for which it is designed. One of the objectives of the proposed framework is to provide a solution space that meets privacy requirements. To achieve this, the framework merges the operations of the privacy protection mechanism with the interaction protocol operations, in an ordered fashion.

By capturing the exposure boundary, it is possible to identify the sensitive information. If information is sensitive, a protection mechanism that can prevent the execution of non-authorized operations is enabled. Therefore, any operation in the interaction protocol that *discloses* sensitive information will be substituted with sequences of operations that include the protection mechanism.

Given the operations in an interaction protocol and protection mechanism operations, every operation in the protection mechanism has been targeted for protecting sensitive information. Therefore, any operations in the interaction protocol that *discloses* the sensitive information will be substituted with the sequence of the interaction operation protraction. Therefore, merging the operations of the privacy protection mechanism with the operations of interaction protocol requires extending the message types and sequences of the protocol. The extension introduces the interaction protocol as a privacy protection-based interaction protocol that integrates the privacy protection mechanism at the interaction level.

Shared information within a set of entities must remain within the given exposure boundary of information in relation to the participant entities. Based on the information that is shared through the interaction protocol within the exposure boundary about a specific entity $e_i$, there is a protection mechanism that can prevent execution on non-authorized operations.

The proposed framework using the provided information at the risk evaluation, PPL evaluation and the interaction protocol reduces the number of possible solutions to only those entities that can provide the expected solution-based privacy protection. By applying the risk evaluation model, it is possible to identify the sensitive information that might be shared among entities in the environment while the messages and sequences of messages among entities construct the interaction protocol of that environment. The framework has the exposure boundary, interaction protocol, PPL evaluation and the type of privacy protection mechanisms that can provide messages and sequences that represent the privacy-based interaction protocol. Entities that adhere to this interaction protocol seamlessly interact with other entities and the interaction protocol applies the privacy protection operations to protect privacy independent from the application. This allows the privacy protection in CDS to be incorporated at the architectural level and to be part of the computation platform.

The operations in the privacy protection mechanism may require a new type of message in the message set of the protocol in addition to an extension on the sequence of the interaction protocol. Through accommodating the privacy protection mechanism at the interaction protocol level, the interaction is limited to entities whose privacy can be protected with an acceptable PPL in their interaction. The sequence of the operations in the interaction protocol is not changed in the privacy-based interaction protocol but the operations of the privacy protection mechanisms are applied. This can prevent or neutralize the execution of non-authorized operations and transforming sensitive implicit information to explicit. Each of the applied mechanisms has a PPL value, and several mechanisms can be integrated with an interaction protocol to form a privacy-based interaction protocol.

## 4.2 Privacy Protection at the Interaction Level

The proposed framework provides the protection mechanisms at the interaction level and extends the interaction protocol with essential messages and sequences to protect the sensitive information that is shared or disclosed in the original interaction protocol.

*Theorem 1: For any incomplete knowledge CDS where entities adopt message-based interaction, the Privacy Model can be adequately addressed at the interaction level* [71].

To provide the supporting materials for the above theorem, it is essential to prove the following points:

- All the information that is shared or disclosed to other entities is decided at the interaction level

- Any class of privacy protection mechanism occurs at the interaction level.

The computation entity in CDS has autonomy on coordinating activities with others. The interaction layer manages the necessary processes to identify the adequate messages to communicate and resolve the interdependency problem. The communication layer is responsible for exchanging messages; however, it does not have the decision-making authority on the messages to be sent and it is not aware of the intent that initiates the exchange of messages.

*Proof:*

*Lemma 1: Let $e_i \equiv < K_i, PS_i, In_i, Com_i >$ the computation entity. For any information $I_{i,r}$ that is going to be shared with $e_j$. $S(I_{i,r}, e_j)$ is decided in $(In_i)$ [71].*

*If* $PS_i$ realizes that to achieve a goal, there is an interdependency problem, $In_i$ finds a coordination solution $CS_i$ with an entity such as $e_j$.

If $(I_{i,r})$ is shared with $(e_j)$

$$\exists I_{i,r}, (I_{i,r} \in I_i^K) | S(I_{i,r}, e_j)$$

There are two possibilities:

1. It is discovered at $PS_i$ that $I_{i,r}$ is required to perform the $CS_{i,j}$ therefore:
$$CS_{i,j} \rightarrow S(I_{i,r}, e_j)$$
2. It is discovered at $In_i$ that $I_{i,r}$ has to be shared with $(e_j)$
$$In_i \rightarrow S(I_{i,r}, e_j)$$

In both cases, the shared information is processed and determined by the interaction layer.

*Lemma 2: Let* $(I_{i,r})$ *be the information that is disclosed. For any* $\left(I_{i,r}\right)$ *there is explicit information that is shared* [71].

$$\exists I_{i,r}\left(I_{i,r} \in I_i^K\right) \mid S\left(I_{i,r}, e_j\right)$$

When information is implicitly disclosed:

$$D\left(I_{i,r}, e_j\right) \to \exists\ I_{i,r'}, o_{j,w} \mid o_{j,w}\left(I_{i,r'}, I^{shr}\ \right)$$

Assuming $I_{i,r'}$ is not *shared* through the interaction. Then there are two possibilities:

1. Fact A: $I_{i,r'}$ is auxiliary shared information $I^{shr}$ disseminated by a third party $(e_t)$ then:

   Using lemma 1:

1. If $\left(I_{i,r'}\right)$ is *shared* with any entity, therefore:

   a. Either $D\left(I_{i,r}, e_t\right)$ so that Fact A occurs

   b. Or it has not been *shared* by an interaction. This contradicts Lemma 1.

This proves that any information that is *shared* or *disclosed* has initiated *sharing* point at the interaction.

In privacy protection, the privacy model is defined as:

$$PP\left(e_j, \left(PS(I_i), \hat{O}_j\right) = \ \forall\ t, w \middle| t \subset PS(I_i)\right)\ \wedge\ \widetilde{\bar{\bar{\hat{o}}}_{J,w\,(t)}^{t}}$$

To achieve $\left(\widetilde{\bar{\bar{\hat{o}}}_{J,w\,(t)}^{t}}\right)$, the privacy protection mechanisms are applied. The privacy protection mechanisms can be classified at the information or operation levels.

*Lemma 3: If a preventive protection mechanism at the information level exists, it happens at the interaction* [71].

Let $(\mu)$ be a preventive mechanism $(\bar{\bar{o}}^{m,D})$ at the information level for protecting $I^s(I_{i,r}, e_j)$ which enables $\left(\widetilde{\bar{\bar{\hat{o}}}^{t}_{J,w\,(t)}}\right)$.

$$\bar{\bar{\mu}} \rightarrow PP\left(e_j, \{I_{i,r}\}, \left(\widetilde{\bar{\bar{\hat{o}}}^{t}_{J,w\,(t)}}\right)\right)$$

$$\mu = < O^{\mu}, I^{\mu} >$$

$$O^{\mu} = \{\, o^{m,1}, \dots, o^{m,d}, \dots, o^{m,D}\}$$

The execution of preventive protection mechanisms at information level sequence order during the interaction. This results in sharing information that is manipulated by the operations in protection mechanisms.

$$\bar{\bar{\mu}} \rightarrow S(I_{i,r'}, e_j)$$

Based on Lemma 1, $(I_{i,r'})$ has to go through interactions. Therefore, the preventive mechanisms at the information level can happen at the interaction level.

*Lemma* 4: If a preventive mechanism exists, it happens at the interaction level [71].

Let $(I_{i,r})$ be the sensitive information that can implicitly be *disclosed* to $(e_j)$ through $(\hat{o}^t_{j,w})$ when $(I_{i,r'})$ is *shared.*

Let $(\mu)$ be the protection mechanism at the operation level that can protect $(I_{i,r'})$. Based on the execution of the protection mechanisms at the operation:

$$\bar{\bar{o}}^{m,D}(\{o_{j,w}, \bar{\bar{o}}^{m,D-1}(\{o_{j,w}, \bar{\bar{o}}^{m,D-2}(\{o_{j,w}, \dots, \bar{\bar{o}}^{m,1}(o_{j,w}, I_{j,r})\})\})\}) = \begin{cases} \emptyset \ \ if \in (o_{j,w}, \hat{o}^t_j) \\ I_{i,r'} \ \ if \ \in (o_{j,w}, \hat{o}^t_j) \end{cases}$$

Which results in sharing $\left(I_{i,r'}\right)$ or $(\emptyset)$. Therefore, based on Lemma 1, privacy protection happens at the interaction level.

*Lemma* 5: if there are punishing privacy protection mechanisms, it happens at the interaction level.

The generated information in this mechanism is *shared* with the entity that has executed the non-authorized operations.

$$\bar{\bar{\mu}} \rightarrow S\left(I_{i,r'}, e_j\right)$$

This indicates that the punishing mechanisms happen at the interaction level.

Given Lemmas 1, 2, 3, 4 and 5, it is proven that any protection mechanisms will be applied at the interaction level. Therefore, capturing the privacy protection at the interaction level can be sufficient.

# Chapter 5

# 5 Privacy Protection Model and Practical Implementation

Introducing the privacy protection model and privacy protection management framework as a computational generic approach that can ensure privacy protection at the interaction level through the interaction protocol. In some respects, the privacy protection model and framework can be utilized as an analytical tool to identify concerns in an interaction protocol and can be incorporated with protection mechanisms [71]. In such an implementation, privacy protection management can be automated in the computation entity or at the computation platform. Any achieved solution at the interaction level requires problem solving and coordination with other participant entities. Thus far, we have proved that to reach acceptable solutions, privacy resolution is essential as computation element at the interaction level.

Our contribution in this work includes designing and developing a privacy-aware computation entity and a privacy protection platform base. In each, the focus is on the computation aspect of the framework that can be practically introduced, thereby introducing the framework elements in the context of practical privacy protection, such as the information categorization, privacy protection mechanisms and exposure boundary of information. The practicality of the privacy protection management framework can affect the implementation of the privacy protection base interaction protocol.

## 5.1 Privacy Protection Concept at the Interaction Level

The main focus is at the interaction level where the computation takes place in addition to the information exchange among entities. As such, the information management becomes an adequate means of molding privacy protection for CDS. Privacy protection is considered during the computation as part of the entity at the interaction level, in which, the interactions are the mechanisms of coordination used to resolve the interdependency problem. Therefore, computation entities can adequately be modeled as (CIR-agents) whereby they have knowledge, problem solving capabilities, interaction, and communication [32][56][71]. The following figure shows the logical architecture of a computation entity.

Modeling the computation entity (CIR-agent) Figure 2: Computation Entity in CDS composed is of Knowledge$(K_i)$, Problem solver$(PS_i)$, Interaction $(In_i)$ and Communication$(Com_i)$. In this information management form of computation, entities are modeled as information and operation.

$$e_i \equiv < I_i, O_i >$$

Knowledge $(K_i)$: conveys all information regarding intentions, belief and states of the entity. This includes information regarding operations that the entity possesses and is capable of applying.

Problem Solver $(PS_i)$: an adjoined layer of the knowledge. It consists of operations to identify goals and required actions towards these achieving this through the information acquired from the knowledge. Because of this, problem solving can be modeled as an operation in information management.

Interaction $(In_i)$: is adjacent to the knowledge, problem solver and communication layers. Through this, the interaction can be modeled as information and operations. The computation entity at the interaction level utilizes a pattern of communication and decision-making to resolve the interdependency problem.

Communication $(Com_i)$: encompasses the messages that will be communicated to other entities, but it does not interfere with coordinating the decision-making processes. The communication layer is modeled as information in information management.

Privacy protection solution as a computation concept are inherently expressed at the interaction level to facilitate a protection-based interaction among participant entities. Applying the proposed privacy protection management framework will incorporate the privacy protection management directly at the interaction level as illustrated in Figure 3, to consolidate interactions with privacy protection management and privacy-based interaction protocol.

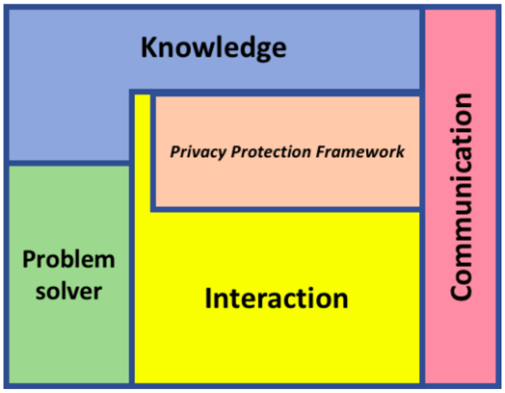


**Figure 3: Privacy Protection at the Interaction**

The interaction protocol consists of a set of messages and each message has a content $C_m$; this content $C_m$ involves sender $e_s$ and receiver $e_r$ entities and operations $O_{s,m}$ that transfer the message.

$$M = \{m_1, \dots, m_m\}, 1 \leq m \leq Z$$

$$m_m =< e_s, e_r, C_m, O_{s,m} >,$$

$$(C_m \in \ I_i), \in \left(O_{s,m} \in \ O_s\right)$$

As was mentioned earlier, the interaction protocols can be modeled as sets of messages $M$ and sequences $S_M$ thereof:

$$IP < M, S_M >$$

Where sequences are constructed by patterns of exchanging messages

$$M^* = \bigcup_{k=1}^{Z} M^k,$$

$$M^*: Allpossible\ sequences\ given\ the\ set\ M.$$

$$M^k: All\ sequences\ of\ M\ with\ k\ lenght.$$

Therefore,

$$S_M = [m_1,\ \dots,\ m_q]$$

$$S_M\ < structure\ of\ ordering\ messages >$$
$$S_M \subset M^*$$

Messages are bound to operations that deliver them. $S_q^o$ represents the sequence of operations:

$$S_q^o = [o_{i,a}, \dots, o_{i,N}],\ 1 \le a \le N$$

## 5.2 Privacy Protection Management Framework in CDS

Privacy protection is a critical aspect in decentralized environments. Entities share information through communication-based interactions. Privacy protection as a computation concept is inherently expressed at the interaction level. Appling the privacy solutions at the computation level, will facilitate interaction among the participant entities in a way that maintains a privacy aware driven interaction.

Interactions in CDS are steered by interaction protocols that can be modeled as messages and sequences of messages. Privacy protection management is responsible for identifying the privacy concerns in interaction protocols and providing a privacy-based interaction protocol that encompasses the protection operations to protect privacy. Incorporating the proposed privacy protection framework as a computational aspect at the interaction level will enable entities to categorize their information in relation with other participant entities and set their exposure boundaries for their information armed with a privacy protection mechanism.

### 5.2.1Information Sensitivity Categorization

Applying the privacy protection framework principles to information $I_i$ will enable the assessment and categorization of that information as either sensitive $I_i^s$, or non-sensitive $\neg I_i^s$ in relation with the other exiting entities in the environment. For whether information is recognized as sensitive or not is determined by the information owner, which is subjective aspect between the information and the participant entities $R^*$. Sensitive information can be captured as the following:

$$I_i^s = \bigcup_{k=1,j=1}^{k\leq N, j\leq W} \left(I_{i,k}, e_j\right) | \; ( e_j \in \left(R^* - \; E_{i,k}\right))$$

Naturally information exists in explicit form, and it can be classified as implicit information when in conjunction with operations. Operations can retrieve the implicit form of information by processing the shared information and turning it into the explicit, and so the classification of information – sensitive or non-sensitive – according to the information utility. Information can be tagged as sensitive information in relation to other entities that could implicitly retrieve new forms of information However, the same information can be tagged as non-sensitive in relation with another group of entities. This demonstrates that not all of the extracted information has a high risk of privacy concerns, as in many case the retrieved information can be non-sensitive. However, in this case, there are no privacy concerns.

Our assumption is that the “information sensitivity” is a subjective aspect in relation with a specific entity. Each piece information is measured differentially with each of the participant entities in the environment $E$. Accordingly, the information $I_{i,k}$ categorization is bounded to information utility, for which categorizing information will demonstrate the state of the Exposure Boundary $E_{(I_{i,k})}$ .

$$I^S\left(I_{i,r}, e_j\right) = \left(e_j \notin \ E_{(I_{i,k})}\right)$$

$$E_{(I_{i,k})}\{e_r, \ldots, e_t, \ldots, e_N\}, E\left(E_{(I_{i,k})} \ \subset E\right), 1 \leq r, t \leq N$$

Any piece of information (I), in order to be categorized it needs to be mapped separately to each participant entity $(e_K)$ in the environment in terms of their operations. The information sensitivity is measured from the Utility (U) model. Capturing the Utility (U) of each piece information with each capable participant entity, then the Risk (R) of sharing information can be identified based on the expected utility $(EU)$. The risk of sharing information is the chance that a negative impact exists, and so the negative impact is modeled as the cost $(C)$ of sharing, and the chance is modeled as probability $(p)$ of the cost potentially incurred

$$C = \left(I_{i,k}, \ e_j\right)$$

$$R = P \times C$$

Capturing the information utility and the probability of occurrence, can give a threshold of the expected utility $(EU)$ and the probability

$$Expected\,utility\ (EU) = Probability\ (p) * Utility\ (U)$$

Given the information related to the expected utility, the system can make a decision despite the incomplete knowledge of the environment. However, this work does not account for those instance in which the system is expected to operate given ignorance of existing entities. the protection under ignorance. The determination of $(EU)$ for each information separately with each participant in a way the sensitivity of the information can be assisted in relation with other participant entities.

The decision-making process of sharing piece information takes place at the entity level. Therefore, the entity can decide whether to accept the chance of a privacy concern by measuring (EU) of the information to decide whether to procced with the interaction or reject it and look for alternatives. This is in direct relation with (EU) and the accepted level of PPL before establishing any interaction. Due to the given proposed information management engine, the categorization process $f_i$ of the information $I_{r,i}$ has demonstrated against each of the participant entities $e_{\forall K-i}$ in relation to information and the entities, expected operations.

$$f_i =< I_{r,i},\ e_{\forall K-i},\ u\left(I_{r,i}, e_j\right) > \ \equiv\ I^s$$

$$e_{K=All\ of\ the\ participant\ entities}\ ,\qquad e_{j=one\ of\ the\ participant\ entities\ in\ the\ environemnt}$$

Signifying the Risk $R$ can produce the boundaries of the shared information. Finding the $EU$ of each piece information with each participant entity can affects an entity's decision. We have categorized the $EU$ of the information at three levels:

$$Risk\colon EU\left(I_{i,j}\right) < 0$$

$$Good\ to\ Share\ and\ no\ Risk\colon\ \ EU\left(I_{i,j}\right) = 0$$

$$Benefit\colon EU\left(I_{i,j}\right) > 0$$

Categorization of any piece of information can be demonstrated differently from one to another entity, whether it is sensitive information or non-sensitive information, as in the following:

- Sensitive information:

$$EU^{-}\left(I_{r,i},\ e_j\right) = I^s$$

- Non-sensitive information:

$$EU^{+}\left(I_{r,i},\ e_i\right) = \neg I^s$$

Estimating the risk of sharing information $I_i$ with $e_j$ among all of the participant entities $e_K$. Where the risk is the compound of the information utility $U$ of the information, and the probability $p$ of the negative impact occurrence.

$$f_i < I_i,\ e_{\forall j-K},\ R > \ \equiv\ I^s$$

$$R = \left(p * u\left(I_{i,j}\right)\right) \leq u\left(I_{i,j}\right),\ where\ (p \leq 1).$$

Replacing the Risk:

$$f_i = I_i,\ e_{\forall j-K}, \left(p * u\left(I_{i,j}\right)\right) \leq u\left(I_{i,j}\right)\ \equiv\ I^s$$

$$where\ (p \leq 1)$$

Since the risk of an interaction is a probabilistic view that associated with the occurrence of negative impact event of privacy concerns on the entity. This allows decision-making processes to evaluate the interaction and assess risk of information sharing that might affect an entity's privacy. As shown in Figure 4: **Information Categorization**.

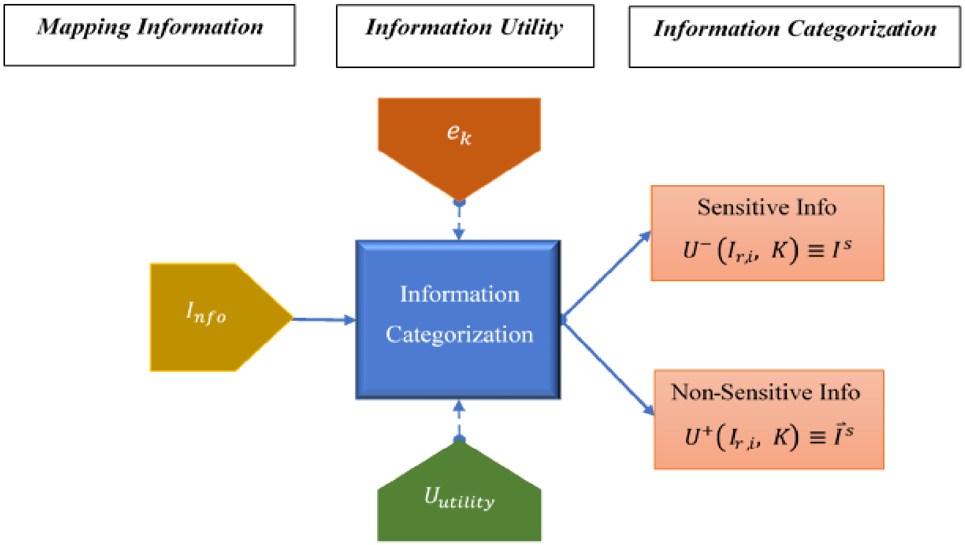

Mapping Information
Information Utility
Information Categorization
$e_K$
Sensitive Info
$U^{-}(I_{r,i},\ K) \equiv I^s$
$I_{nfo}$
Information Categorization
Non-Sensitive Info
$U^{+}(I_{r,i},\ K) \equiv \vec{I}^s$
$U_{utility}$

**Figure 4: Information Categorization**

As was earlier mentioned, information categorization is a relative aspect that can be measured differently for each participant entity $(e_i)$ in relation with the information that is to be released $I_{r,i}$. Since the open environment is imposing some limitation on the participant entities, the proposed information categorization engine needs to be practical assessed in a way that it can efficiently adopt the environment setting. Efficiency is illustrated from the scope of time complexity of the information categorization engine $f(I_i)$.

In this section, the time complexity of the proposed information categorization engine $f(I_i)$ is captured for each $I_{i,j}$, powered by each participant entity $e_K$. The information categorization demonstrates that complexity is governed by the growth of the input $(n)$, which is in this case the number of participant entities and evaluated information. Given the previous analysis, the time complexity can be demonstrated as an exponential growth $O(n)$ that can be affected by the increments of the entities $(k)$ that need to be evaluated against each information utility $U$ evolution $(m)$ in order to be categorized for $(n)$ rounds. Thus, the growth of the worst-case complexity is correlated to the incremental size of the input, which is the potential entities:

$$\mathrm{O}(n * m * k)$$

Each piece information needs to be mapped to the provider entity in the context of the expected utility. From a practically perspective, the concept of information mapping is considered practically attainable in the context of an open environment.

### 5.2.2 Exposure Boundary Identification

Privacy in the context of information management is the state of exposure boundary $E_{i,k}$ of information $I_i^k$. Exposure boundary $E_{i,k}$ includes only entities that can share information with each other. Each computational entity has all information, intentions, belief as well as the exposure boundary of its' information as part of its knowledge.

$$\left(I_i \subseteq I_i^k\right), \forall k\left(E_{i,k} \subset \; I_i^k\right)$$

Information is shared in an interaction protocol through messages $m_m$ by capturing the sender $e_s$ receiver $e_r$ entities of the messages in the interaction protocol.

$$m_m =< e_s, e_r, C_m, O_{s,m} > ,$$

$$O_{s,m}: operaton\ of\ sending\ , C_m: Content, \in (C_m, I_i), \in \left(O_{s,m}, O_s\right)$$

Therefore:

$$e_K = \bigcup_{\forall s,r} \{e_s, e_r\} | < e_s, e_r, C_m, O_{s,m} > \in M\ ,\ e_K: All\ participant\ \ entities$$

Introducing the privacy protection at interaction level as it is shown in Figure 3: Privacy Protection at the Interaction Level, will adequately allow us to inject the privacy protection management framework. Equipping a computational entity with the proposed privacy protection management framework will enable sensitive information categorization and its exposure boundary and the required privacy protection mechanism to maintain privacy protection. By applying the privacy protection framework, the entity will be privacy aware-based as it presented in  Figure 5 Privacy protection aware entity.

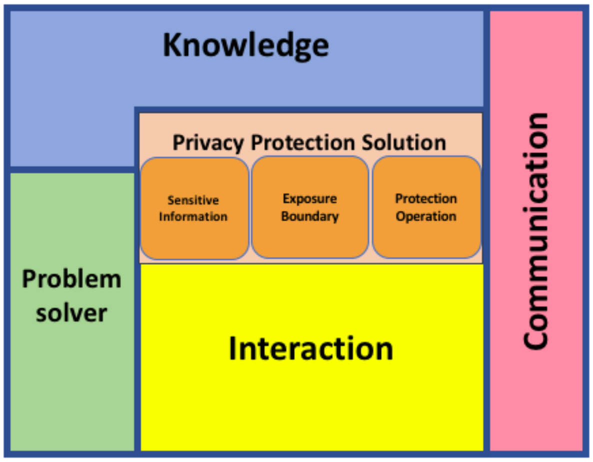


**Figure 5: Privacy protection aware entity**

Accordingly, this framework classifies the information into two forms, explicit and implicit. The implicit form of information is a conjunction of explicit information and operations. This shows that the privacy concern is mainly governed by information transformation from one form to another by applying operations. Such operations become non-authorized operations. Exposure boundary $E_{i,k}$ is utilized by an entity to decide if other entities that exist in the open environment are in its exposure boundary or not in relation with their information.

$$E_{i,k} = \{e_{i,t}, \dots, e_{i,N}\}, (E_{i,k} \subset E), 1 \leq t \leq N$$

Participant entities do not have complete knowledge about the existence of others in the environment. This lack of knowledge restricts entities in identifying $E_{i,k}$ information in relation with potential participant entities. Consequently, this imposes a practicality shortage in identifying $E_{i,k}$ in the open environment. However, the $E_{i,k}$ is strongly coupled with the categorization information.

In this analysis, the exposure boundary identification concept is measured from the practicality implementation side, in which the exposure boundary classifies the potential entities into two groups – “with-in” or “out-of” – the exposure boundary of the entity up on the produced utility.

Giving $E_{i,k}$ will index all participant entities that classify the participant entities given their operations in relation with the released information. This demonstrates that the information – sensitive or not – is a relative concept and not an absolute one. Entities will be mutually exclusive in respect to their relation with the shared information $I_{r,i}$. The information sensitivity in relation with others, implicitly introduce the concept of the $E_{i,k}$

$$E_{i,k} = \{e_{i,t}, \dots, e_{i,N}\}, (E_{i,k} \subset E), 1 \leq t \leq N$$

$$I_{r,i}: e_{i,k} \cap e_{j,k} = \phi$$

$$e_k : e_{i,k} \cup e_{j,k}$$

The exposure boundary $E_{i,k}$ concept needs to be practically identified in the context of the open environment. Such an implementation is required to capture information utility that can demonstrate the boundary of each piece information in relation with the participant entities $e_K$. The entity's exposure boundary can be structured by in which time that the outcome of the shared information utility introduces the categorization of the information in relation with all of the participant entities $U^+\left(I_{r,i},\ K\right)$.

The exposure boundary of an entity will be constructed and demonstrated to consider whether a set of entities is "IN" or "OUT" of the entity's boundary

$$\boldsymbol{Within\ the\ Exposure\ boundary}\text{: } E_{i,k}\{k_i\ |U^+(I_{r,i}, k_i\}$$

$$(j \neq i)$$

$$\boldsymbol{Out\ of\ the\ Exposure\ boundary}\text{: } E_{I_{i,k}}\left\{k_j\ \middle|U^-(I_{r,i}, k_j\right\}$$

Any entity will be out of the entity $e_i$ exposure boundary $E_{(I_{i,k})}$, if information has been categorized as sensitive $\neg I_i^s$ in relation with a specific entity $e_j$.

$$\neg I_i^s = \left\{E_{(I_{i,k})}\ -\ e_j\right\}$$

The exposure boundary of an entity $E_{i,k}$ is a subset of the all existing entities in the environment $E$.

$$\vec{E}_{i,k} =\ \left\{E\ - E_{(I_{i,k})}\right\} \text{ the index of } I_{r,i}$$

**Figure 6** shows information exposure boundary identification:

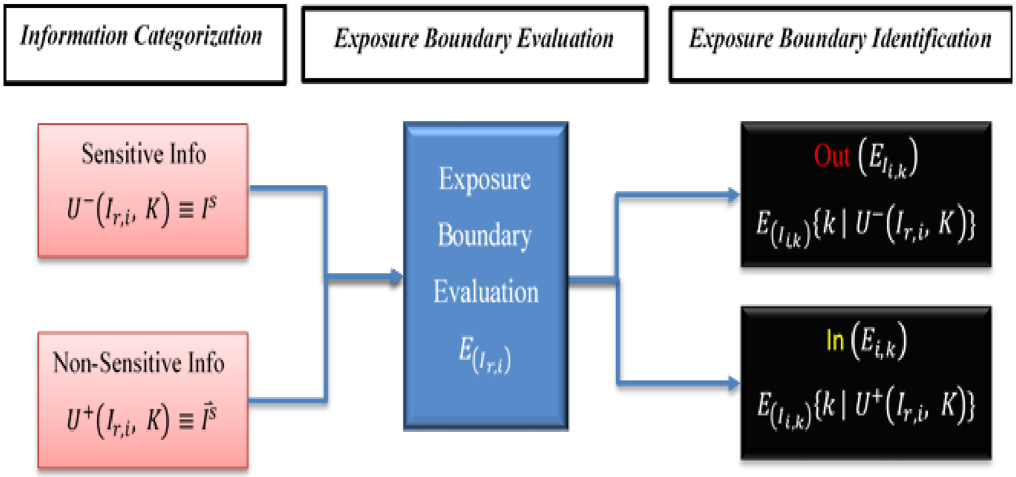

Information Categorization
Exposure Boundary Evaluation
Exposure Boundary Identification
Sensitive Info
$U^{-}(I_{r,i}, K) \equiv I^{S}$
Non-Sensitive Info
$U^{+}(I_{r,i}, K) \equiv \vec{I}^{S}$
Exposure
Boundary
Evaluation
$E_{(I_{r,i})}$
Out $(E_{I_{i,k}})$
$E_{(I_{i,k})}\{k \mid U^{-}(I_{r,i}, K)\}$
In $(E_{i,k})$
$E_{(I_{i,k})}\{k \mid U^{+}(I_{r,i}, K)\}$

**Figure 6 Information Exposure Boundary Identification**

The exposure boundary efficiency is introduced in the time complexity aspect. Time complexity is an approximation when an algorithm detects a termination point with respect to a solution, where the complexity is an abstract model that can be applied to any measurement. In this analysis, it has proportioned to time complexity $O(n^2)$ the boundary complexity efficiency is measured based on the size of the space that an entity can be exposed to and the complexity behind the number of the participant entities. Correspondingly, the complexity source of the exposure boundary is correlated and driven by the complexity of the information categorization, where the exposure boundary is neutrally specified by the information categorization and that illustrations that the exposure boundary identification complexity itself is:

$$O\left(E_{(I_{i,k})}\right) = O(n)$$

**Figure 7.** Information Categorization Management Engine illustrates the overall information categorization engine:

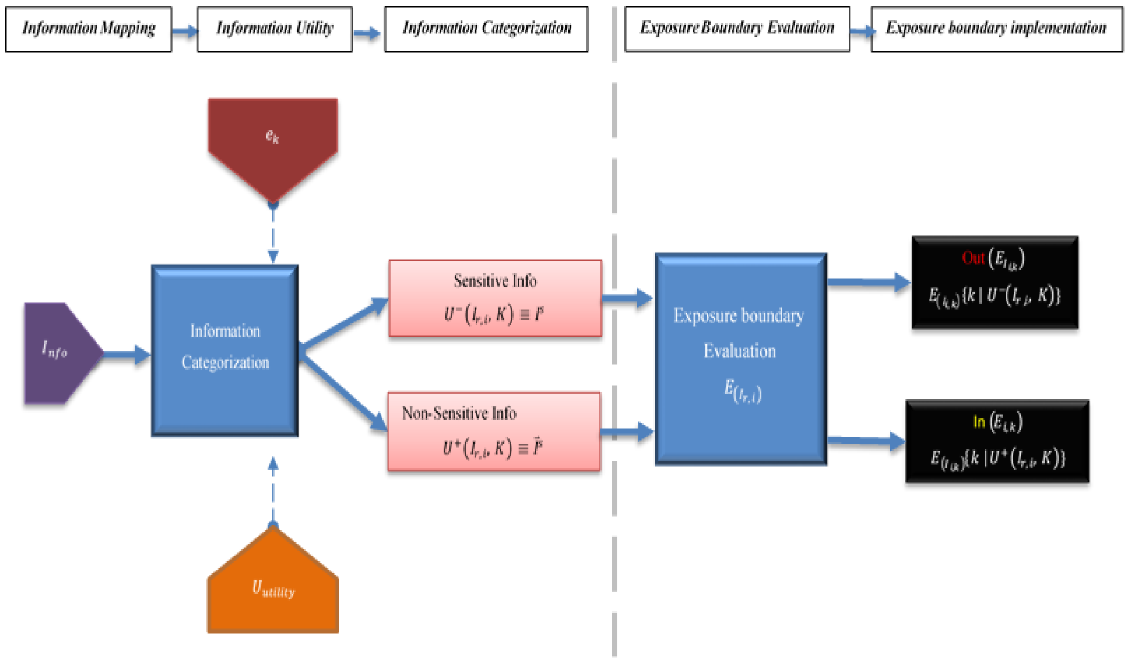

Information Mapping
Information Utility
Information Categorization
Exposure Boundary Evaluation
Exposure boundary implementation
$e_k$
$I_{nfo}$
Information Categorization
$U_{utility}$
Sensitive Info
$U^-(I_{r,i}, K) \equiv P$
Non-Sensitive Info
$U^+(I_{r,i}, K) \equiv \bar{P}$
Exposure boundary Evaluation
$E_{(I_{r,i})}$
Out $(E_{I_{i,k}})$
$E_{(I_{i,k})}\{k \mid U^-(I_{r,i}, K)\}$
In $(E_{I_{i,k}})$
$E_{(I_{i,k})}\{k \mid U^+(I_{r,i}, K)\}$

**Figure 7. Information Categorization Management Engine**

### 5.2.3 Privacy- Based Interaction protocol

An interaction protocol $(IP)$ is a structure that combines messages and their sequences. Where the interaction protocol follows a sequence of messages $(M)$ and operations $(O)$ among entities to deliver a content from one entity to another. $IP$ has been modeled as sets of messages $(M)$ and sequences $(S_M)$.

$$IP =< M, S_M >$$

Applying proposed privacy protection management frameworks as a computation aspect and incorporating privacy protection management directly at the interaction level insures that the privacy concerns that can be carried within the interaction protocols can captured

$$IP =< M, S_M >$$

$$M \equiv \{m_1, \dots, m_m\}, 1 \leq m \leq Z$$

$$m_m \equiv < e_s, e_r, C_m, O_{s,m} > ,$$

$$e_r: Receiver \ \ , e_s: Sender, C_m: Content, \in (C_m, I_i), \in \left(O_{s,m}, O_s\right)$$

Released messages $M^k$ can contain an information that is carried over during the interaction, where this message is passed through a specific set of sequences $(M^*)$, which are constructed by patterns of exchanging messages

$$M^* = \bigcup_{k=1}^{Z} M^k$$

$$M^*: Allpossible\ sequences\ given\ the\ set\ M.$$

$$M^k: All\ sequences\ of\ M\ with\ k\ length.$$

Therefore,

$$S_M = \left[m_1,\ \dots,\ m_q\right]$$

$$S_M \ < structure\ of\ ordering\ messages >$$
$$S_M \ \subset M^*$$

The privacy concerns in the interaction protocol have been captured from message content that might carry an information $I_{i,k}$ that is considered sensitive to be exposed. This information is exchanged through the messages $M$ and their sequences $S_{q,t}$. Therefore, evaluating sequences $H_i^*$ of the interaction protocol to identify shared sensitive information is essential in relation with participant entities $e_j$.

$$H_i^* \equiv \bigcup_{q=1,j=1,t=1,k=1}^{q\leq Q,j\leq w,t\leq T,k\leq N} \left(S_q, I_{i,k}\right) | \left(= (\bar{\bar{\bar{S}}}_q^o\ (M), I_{i,k}\right)\ \hat{}\, I^s(I_{i,k}, e_j))$$

Introducing the proposed privacy protection-based framework at the interaction protocol will extend only the necessary points in the interaction that might lead to a privacy concern. In this respect, privacy protection will be maintained during the interaction, since the messages and sequence will be privacy-protection based. Also, the shared information $A_i^*$ will be another concern that might disclose the sensitivity of the shared information. The shared information by itself is considered non-sensitive information, but it can be used as auxiliary information to transform implicit sensitive information to explicit.

$$A_i^* = \bigcup_{q=1,j=1,t=1,k=1}^{q\leq Q,j\leq w,t\leq T,k\leq N} \left([o], I_{i,k}\right) | \left(= (o, \bar{\bar{\bar{S}}}_q^o)\ \hat{}\, \bar{\bar{o}} = S(I_{i,k}, e_j)\right)$$

The practicality aspect of the new privacy protection-based interaction protocol ($PB\_IP$) is a critical point of validation. The practicality is determined by the behavior of the interaction protocol after the extension, which should maintain the same performance as the original protocol toward achieving a task. Yet, the solution will be a privacy protection based. The privacy protection-based protocol ($PB\_IP$) needs to maintain the outcome of the original protocol that it has been designed for. Applying the proposed privacy protection framework through the interaction protocol will turn the sequences into $PB\_Sm$, so as to narrow down the existence of others to only those entities that can maintain the privacy protection. In a way, privacy protection requirements will be imposed as a constraint in any proposed solution. Also, the termination of the utilized interaction mechanisms after applying the privacy protection framework is a crucial point in demonstrating the practicality of a proposed ($PB\_IP$):

$$PB\_IP = <\ PB\_M, PB\_Sm\ >$$

### 5.2.3.1 Privacy Protection-Based Interaction Protocol Termination

In the interaction protocol the released messages can contain a set of details that are carried over during the interaction. Therefore, the message has to specify the sender and the receiver, which defines the flow of the messages. Additionally, the messages flow through sequences. The sequences orchestrate the pattern of the messages during the interaction, which impose the order of the message flow.

$$IP =< M, S_M >$$

$$M = \{m_1, \ \dots, \ m_m \}, \ 1 \leq m \leq Z$$

$$m_m \ =< e_s, e_{m,} C_m, C_{s,m} >, \ (C_m \in \ I_i), \left(O_{s,m} \in \ O_s\right)$$

$$S_M = \left[m_1, \ \dots, \ m_q\right]$$

$$S_M \ < structure \ of \ ordering \ messages >$$

During the process of assignment utilizing the $PB\_IP$, only the potential contractor who is capable of handling the requested task within a specific privacy protection constraint will be assigned. In such process the interaction protocol can get into an iteration process until it finds the required maximum value. For instance, the service requester will look for which one of the participants is the best to deliver the maximum value of the requested task. Accordingly, the winner provider is determined and the termination point of the protocol.

The interaction protocol is designed to resolve the interdependency problem in the interaction, to reach the desired solution among distributed multiple entities. Therefore, the complexity behind the termination process is determining to be the “Best” potential provider which can provide the requested solution to the assigned problem. By introducing the concept of “Best”, the problem has been transferred to an optimization problem. By natural, the optimization problem is (NP-Hard problem), and any interaction protocol has an optimization problem. Naturally, in distributed space any interaction protocols such as assignment protocol and negotiation protocol, they have an (NP-Hard problem) by default in the open environment. The optimal solution for an “optimization problem” is finding the best “optimal solution” in an open environment. In such distributed space, there is no centralized entity that has global knowledge about all the solutions that do exist in the space. This demonstrates that a solution is distributed among the participant entities in the space, each entity exposes part of the solution and entities need to negotiate to deliver the requested solution.

The solution is exposed incrementally since there is no entity that has the overall knowledge about all the participants who can help in such a space distributed naturally. Therefore, the utilized interaction mechanism is the optimization problem of a distributed space, where they are (NP-Hard) in general. Alternatively, utilizing a heuristic solution will be acceptable for decentralized distributed space setting. Since the interaction protocol is correlated to the interaction mechanism, the interaction mechanism will decide when the protocol can be terminated. Nevertheless, the is approximate or near to optimal solution would be acceptable, in which the approximate is better than random, as such the heuristic solution is adopted.

#### 5.2.3.2 Privacy Protection Interaction Protocol Outcome

Applying the privacy protection management framework on interaction protocols allows us to identify the privacy concerns at the interactions. It evaluates the messages and sequences and provides adequate protection operations within the interaction protocol that result in privacy-based interaction protocol (PB_IP). The extended privacy-based interaction protocol is generated by applying the privacy protection management framework. The privacy-based extension does not affect the overall feasibility of the original interaction protocol it still reaches the same outcome of the original interaction protocol before applying the privacy protection framework. However, any solution that was not achievable before the privacy protection extended protocol will not be attainable after introducing the privacy protection protocol. Not all of the feasible solution that are reached before the new extinction remain feasible after applying the framework. Not all of the available solutions will meet the privacy protection criteria after applying the privacy protection extension. This makes it infeasible to reach all of the available solutions that were available before the privacy protection extension.

The privacy protection management framework introduced the privacy protection requirement as constraint variables in the solution space. In a way, any potential solution that does not meet the privacy protection constraints will not be accepted. Consequently, the solution space will be restricted only to the solutions that can solve the capability interdependency issue and at the same time can handle the privacy preference among all of the available solutions. Despite the fact that a solution space of an interaction protocol before and after the framework extension has shrunk, any legitimate acceptable solutions at the computation level require the inclusion of privacy resolutions for problem-solving and coordination.

One of the main points that drive the practicality analysis is the attained outcome of the interaction protocol before and after applying the privacy protection framework. The solution outcome that can be attained after implementing the privacy protection base interaction protocol should maintain the same original outcome. The privacy-based interaction protocol is handling the same issue that the original interaction protocol was dealing with. Yet, consider the privacy protection as a constrain of any solution.

The $PB\_IP$ is feasibly applied as a base for any privacy protection interaction. However, the new privacy-base protocol is carrying a level of complexity. This complexity source of the PB_IP yelled by the termination aspect of the interaction protocol. The termination is driven by the interaction mechanism that the framework has introduced to it.

#### 5.2.3.3 Privacy Protection Interaction Protocol Practicality Analysis

The Privacy Protection Interaction Protocol ($PB\_IP$) has different levels of complexity depending on message redundancy. The first complexity level is the time complexity per message, which is based on the number of participants receiving the message flow to. As such, it is measured by the number of repeated process for each message with each participant that will result a Linear growth complexity. The second and most importantly source of complexity is the termination of the interaction. The combination of all the messages, sequences and the termination will demonstrate the overall complexity. Our analysis of the interaction protocol will be divided into two main complexity levels, per-message and overall protocol time complexity.

Messages flow in a certain sequence, a flow that delivers the exchanged messages between entities. Each message might have a different order of sequence than others. Each message in the interaction protocol conveys content $C_m$ and a sequence $S_M$ to deliver this content.

$$m_m \ \equiv < e_s, e_{m,} C_m, C_{s,m} >, \ \in (C_m, \ I_i) \in \left(O_{s,m}, \ O_s\right)$$

Sequences are constructed by patterns of exchanged messages. There is a specific list of sequence $(\mathrm{Order})$ of messages $(M)$ to follow to deliver an expected outcome of a certain type of message.

$$S_M = \left[m_1, \ \ldots, \ m_q\right]$$

$$S_M \ < structure \ of \ ordering \ messages >$$

The sequence structure is ordered as a (List pattern), which is not a (Set pattern), where the flow in the (Set pattern) does not follow a parallel sequence. Yet, it has a set of orders that can follow a specific pattern of sequences. In order for the messages to be delivered, there will be operations that interfere with delivering this set of messages among the participant entities. The carried-on complexity in the original sequence of the interaction protocol is introduced by the delivery of the expected outcome that an interaction protocol meant for. This is captured at two main levels aspects of complexity – per-message complexity and set of messages complexity.

Messages need to flow from the service requester $(e_s)$ to the service provider $(e_m)$ which will initially remain (Linear Growth $O(n)$) throughout the process of the interaction. The same pattern will remain during the message delivery. However, complexity can be affected by the increments of providers $(e_m)$ and the number of the flowed messages $(M)$ between them. The initial state of the growth is (Linear Growth $O(n)$), and it can be impacted by a change it message number. The cycle of complexity growth is yielded for each round, with each provider and each message in the two stages of classification. The overall complexity for each message can be demonstrated as $\big(O(n)\big)$. This complexity is considered the lower bound for each of the two levels – message level and sequence level – that the message can generate during the interaction cycle.

Capturing the pattern complexity that each message can go through during the interaction at two levels will be illustrated, where it is measured in the context of the overall communication of the interaction protocol. Our focus is mainly on the complexity behavior when the "input size" increases with the interaction protocol. Input is modeled as the participant entities / messages (the sequence). The overall complexity of the interaction protocol will be mainly related to the overall message complexity and overall message sequence complexity. The overall message complexity stage is correlated with the number of the input messages during the interaction, where the lower bound complexity increases with the increment of the potential provider complexity and this demonstrates the Linear growth of the complexity behind all messages $\big(O(n)\big)$. Meanwhile, the overall messages sequence complexity at this stage is the lower bound the complexity demonstrate $\big(O(n)\big)$ as well, since the growth of the complexity is related to the growth of the message in which the number of the sequences are fixed.

The last stage the interaction protocol analysis is the overall protocol termination and privacy solution determination complexity. The investigation is mainly about marking the end point of a protocol that demonstrates the complexity of the protocol functionality. Some protocols' complexities are exponential, as they are as cyclic as the nature of the protocol, whereas a protocol can get into a $(loop)$ that results in a protocol that is impractical, inefficient and not feasible; this can be different from one to another interaction mechanism. Loop represents an exponential complexity growth, in which it creates nondeterministic polynomial time (NP), if it presents a cyclic pattern "$loop$". Accordingly, all mechanisms have their own distinct termination complexities, which are not an absolute aspect for all of the interaction mechanisms.

The complexity is investigated overall on three levels: Message level, Sequence level and Termination level. Complexity growth occur on the Message level and at the Sequence level, but it is introduced as leaner growth overall on each of the levels. The complexity of the Termination is captured from the protocol capability to solve the interdependency problem without involving in an "endless loop", while the protocol message sequence is preserved in this original form. However, the conversion of the operation is repeated until it achieves the expected solution. As such, this makes the interaction protocol an expensive solution that would not be practical as an optimal solution, where what is produced has exponential complexity growth. There are interaction protocols leaner by structure, as they are not cyclic. For example, any form of list structure is considered *Leaner*. However, if one of the nodes returns to one of the previous nodes, it would be considered cyclic and the protocol would be a potential *Exponential.*

## 5.3 Practical Privacy Protection Computation Based

This work has introduced the proposed solution at two levels. The first level deals with the main proposed privacy protection framework elements in practical terms, where the proposed practical elements aspect has been introduced in the beginning of this chapter and each of the elements has been introduced in a practical context. The second level is practical computation-based privacy protection architecture. The key point of this level is the practical privacy protection-based solution toward the computation aspect implementation of the privacy protection-based framework, which can be illustrated from the entity level and / or the platform level. As such, the lens of the practicality that is carried is the efficiency and feasibility aspects. By establishing the architecture aspects, whether at the entity or platform level, the practicality of the proposed framework will be maintained. As such, the proposed assumption is that the environment capability will be extended with the privacy protection property, and so will be a privacy protection centric environment.

Going forward with the given analysis, it is practical to introduce the proposed framework in an open environment where a limitation has been imposed by the nature of the environment itself. Therefore, one of the proposed solutions is to elevate some of the framework elements to be held by the platform itself. The proposed solution would not be practical if the feasibility behind it has not been demonstrated, where the feasibility can illustrate the ability of implementing such a solution in an environment is open by nature. In this work, the feasibility will be assessed from the implementation of the Privacy Protection Framework. The proposed solution will not be considered practical if it is not feasible to demonstrate it at each of the mentioned computation architecture levels, where the feasibility can illustrate the ability of implementing such a solution in an environment that is open by nature. Carrying on the practical properties of the Privacy Protection Framework, we elevate some of the framework elements to the environment itself, which is the platform level, and the rest will remain at the entity level. In such a scenario the complexity of the proposal will be measured partially at the platform and the other framework complexity will be carried at the entity level itself, and this will be demonstrated and elaborated on it within the details following the proposed solution.

## 5.4 Privacy Protection as an Architecture Computation.

Introducing the privacy protection computational concept as a base of interaction for the participant entities will allow any entity that has joined the space to be privacy protected by default. Due to the fact that entities in CDS have an interdependency problem for which they need to interact in order to reach achieve their goal. The computation entity within CDS can adequately be modeled a CIR-Agent that has knowledge, problem solving capabilities, interactions and communications. Introducing part of the practicality architecture aspect as a computation element at the entity and / or at the platform can bound the impracticality deficiency introduced through the proposed framework implementation. As such, the practical implementation of the privacy protection can be achieved in conjunction with problem solving and a coordinated solution, which can be managed by interactions. The privacy protection interaction can be partially carried out by the platform. By applying the framework, any solution that is achieved will not be acceptable if the privacy concerns are not resolved. This can carry a cost of complexity that is introduced when applying the framework, especially if carrying the proposed framework can impose a burden on the participant entity, as it will not be practical at the entity level only.

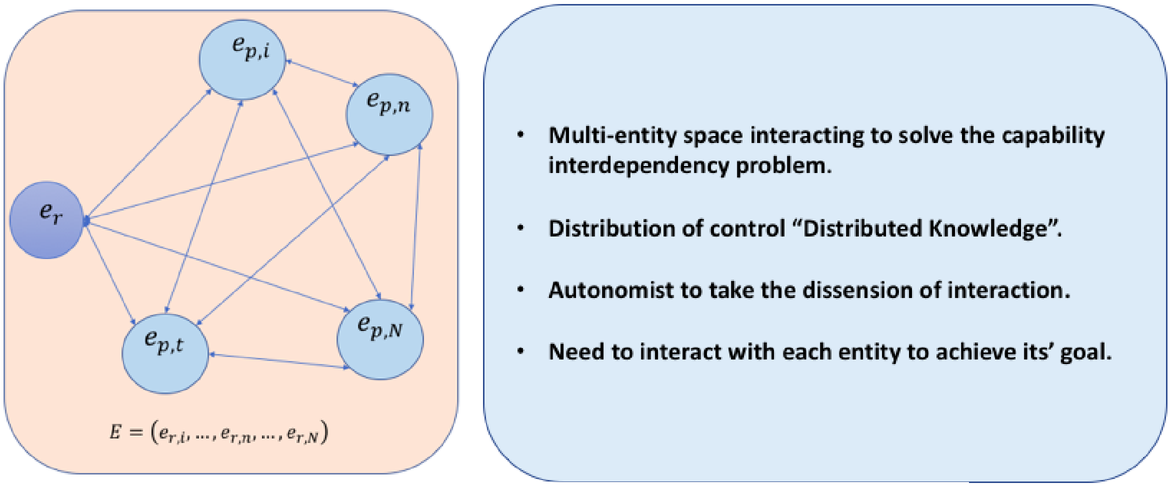
The privacy protection management framework is applied at the computation level by expanding the structure of the computational entity and the computational platform. The privacy protection is given through the collaboration of both of the entities and platform protection elements. In this dissertation, we have demonstrated a legitimate acceptable solution at the computation level that requires the inclusion of a privacy resolution in addition to the problem-solving and coordination through the interaction adhering the privacy protection-based interaction protocol. Elevating part of the proposed framework to the platform level in order to carry the practicality deficiency burden, if there is any yielded by any of the main framework elements' implementation.

The proposed privacy protection framework needs to be partially carried at the platform, and the rest at the computational entity by extending the interaction part of the computational entity and implementing it at the computational platform as well. The comprehensive analysis of the proposed framework main elements, will demonstrate the results of the practicality of each element, with the result that the practicality aspects of the framework elements will identify which part can carry a complexity cost in the context of communications and computations that need to be elevated to the platform level.

### 5.4.1Communication and Computational Complexity

The implementation of the privacy protection framework within a specific architecture can reduce the practicality complexity, since the nature of the open environment imposes an impracticality aspect that makes the implementation in certain architectures inefficient, difficult and imposes a communication impracticality aspect.

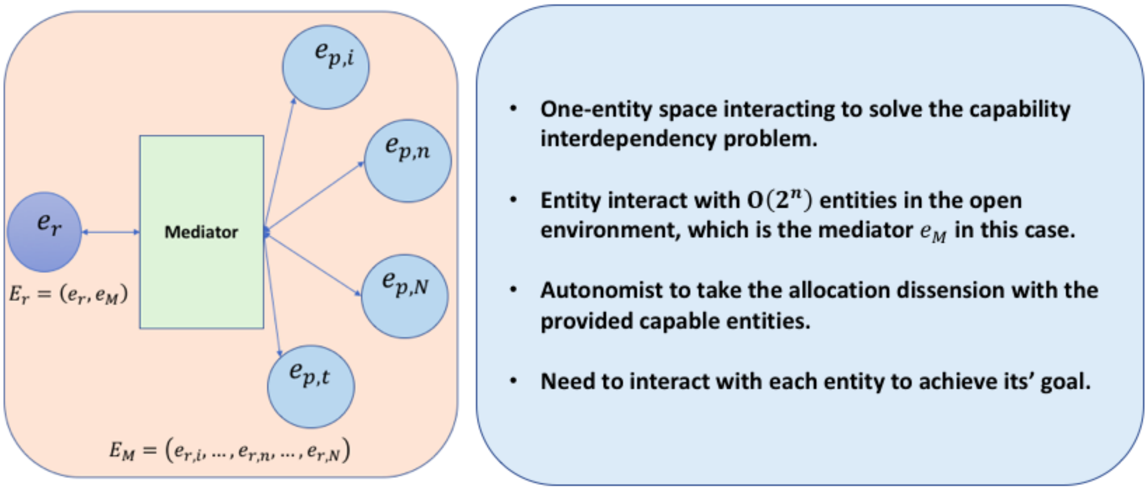
Equipping an entity with a privacy protection alone will not solve the impracticality issue of the communication complexity deficiency per-say. As such, if the entity is privacy-protection aware but it still needs to interact with each existing entity in the environment to solve its capability interdependency problem, in such an implementation, the framework will be an overlap that limits an entity capacity against unpredictable capable participant entities in the open environment in order to solve the interdependence problem. This will add another level to the communication complexity among the participant elements as it is demonstrated in Figure 8: Interaction among entities in open environment.



- **Multi-entity space interacting to solve the capability interdependency problem.**
- **Distribution of control "Distributed Knowledge".**
- **Autonomist to take the dissension of interaction.**
- **Need to interact with each entity to achieve its' goal.**

**Figure 8: Interaction among entities in open environment**

The communication complexity behind the previous architecture implementation is resolved by introducing the mediator approach architecture. The Mediator, as shown in Figure 9, is a plug-in entity, which is the first point of contact for all request by potential providers. The mediator architecture practically resolves the capability interdependency in an open environment setting where requester entities are distributed, and they do not have a complete knowledge of the environment and the potential capable providers.



- **One-entity space interacting to solve the capability interdependency problem.**
- **Entity interact with $O(2^n)$ entities in the open environment, which is the mediator $e_M$ in this case.**
- **Autonomist to take the allocation dissension with the provided capable entities.**
- **Need to interact with each entity to achieve its' goal.**

**Figure 9: Mediator architecture in open environment**

In this work, the concept of the mediator has been adopted and introduced in the context of the platform. The broker in our solution is one of the scenarios and has nothing to do with the privacy protection and the proposed framework, where the broker itself has only one functionality, which is a mapping mission, mapping the request to the potential provider "capability". Nevertheless, the platform will be the base of interaction for any service and potential entity that participates in the space, which implies the privacy protection at the platform architecture is a computational aspect, that can be imbedded is an extension base of the platform in a way that the interaction becomes to be a privacy-based interaction. By the time that any of the participant entities decide to utilize any of the available services that live at the interaction platform, they will collaboratively interact with each other through the privacy protection-based platform. The services, such as broker or scheduler, do not affect the platform functionality per-say since all the mentioned services are reached through the privacy protection-based platform and they will have their privacy protection assessed before delivering any service.

As a result of this investigation, the privacy protection was adapted through the platform in a way that framework will be the base of interaction and an analytical tool containing sets of formulated concepts that are essential for evaluating the state of privacy in computational systems as shown in Figure 10: Privacy Protection Base Platform.

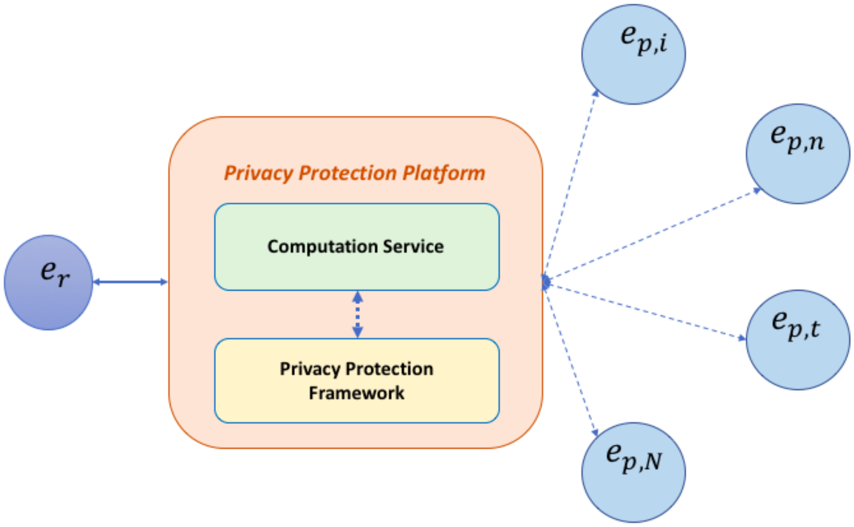


**Figure 10: Privacy Protection Base Platform**

Applying the privacy protection-based platform architecture in the open environment utilizing the privacy protection management framework (PPF) principles, the exposure boundaries and sensitive information for each entity will give the strict criteria that will govern the interaction process, since in open environments entities do not have complete knowledge about communicated information as well as all operations in other entities. This demonstrates the necessity of capturing the privacy protection as an essential property at the computation level and providing protection mechanisms required to incorporate privacy protection during the interactions.

The communication architecture complexity will be bounded at two levels, the platform level and entity level. The proposed privacy protection framework is partially carried out at the computational platform, in a way such that the burden of interaction facilitation and privacy mechanisms engine will be handled at the platform. As such that, the privacy protection is considered a base for any interaction in a way no interaction will be established if it does not meet the privacy protection metrics that measure the protection level, where the privacy protection metrics are governed by the participant entity utility. Information utility is given by the entity and the privacy protection is provided by the platform. Accordingly, the communication complexity will be reduced to the level that the entity will carry the complexity of identifying the information utility and the platform registration and interacting with it, whereas the task allocation is based on the privacy protection according to the given entity preference.

At the computational platform, the interdependency problem is classified as capability interdependency and the interaction device is the “assignment”. The capability mapping is one of the platform’s main functionalities that maps the requester entities to the capable requester providers who can consent to the privacy protection requirement that is imposed by the privacy protection platform extension. From the privacy protection implementation point of view, by applying the privacy protection as a base at the computational platform, the computational entity does not need to handle privacy protection techniques implementation. Yet, the information categorization and information exposure boundary identification are the participant entity duty to be handled.

The proposed assumption will deliver the privacy protection-based platform as a trusted universe. Nonetheless, the setting of the applied platform is assumed to trust what governs the privacy of the participant’s entities. Such a setting is not necessarily that both of the other two sides of the entities are not trusted where the platform carrying the necessary privacy point of the attended entity is based on their applied preference Also, this approach can be attainable in all CDS environments and their privacy models. The proposed platform architecture provides an appropriate separation of responsibilities, allowing entities to focus only on achieving their goal under the privacy protection umbrella that has been introduced by the platform that models the solution and solves their problems without carrying the privacy concepts of the privacy.

The Practicality of the proposed solution has been demonstrated as: *Feasibility* and *Efficiency*, for which the feasibility of the proposed solution is introduced in the context of environment expansion, where the environment what we refer to as the platform, has been extended with privacy protection engine impeded in a way such that handles part of the proposed framework as a base of the interaction. Maintaining the main platform computational functionality after the framework extension is demonstrating the feasible of the proposed solution. On the other hand, efficiency is measured interims of the participant matching and task allocation complexity. Separating the responsivity by elevating the matching responsibility from the entity level to a platform level will reduce the complexity to a level $O(1 * n)$ such that elevation, participating entities will not need to interact with all of the participate entity in the environment, but it will only need to interact with the computational platform $O(n)$. The platform will carry all the heavy computational load, such as the capability matching and task allocation, while carrying the privacy protection mechanism engine.

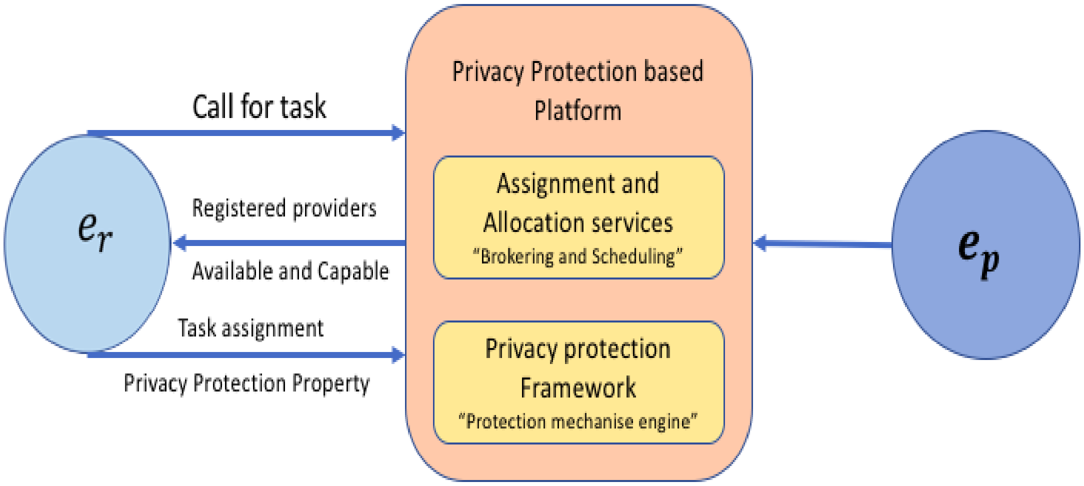

Call for task
Registered providers
Available and Capable
Task assignment
Privacy Protection Property
$e_r$
Privacy Protection based Platform
Assignment and Allocation services
"Brokering and Scheduling"
Privacy protection Framework
"Protection mechanise engine"
$e_p$

**Figure 11: Privacy Protection based Platform**

Figure 11: shows that the requester entity $e_r$ assign the task to the potential participant providers $e_p$ based on its privacy protection preference that has been calculated through the proposed privacy protection engine in relation with the potential providers.

### 5.4.2 Computation Architecture Implementation

At this point, the privacy protection is geared toward providing a computational privacy protection-based system throughout a computational entity and computational environment modeled as CDS. In this dissertation, several key contributions and their implementation have been practically assessed. As such, capturing the practical implementation of the privacy protection framework (PPF) at the interaction level as a computational aspect. Introducing the privacy PPF as a computational element will reduce the potential interactions and shrink the solutions space to the level where only the participant entities who can meet the privacy protection requirement can be selected. The PPF implementation was established at two levels, the platform level and the entity level. The privacy protection at the platform will provide a privacy aware computation system, and at the entity level will transform any participant entity to a privacy-aware computation entity. In order to build a privacy protection environment, the proposed PPF has been adopted as a modular architecture that is utilized as a base of interaction among participant entities this present in the open environment will maintain their privacy protection. This proposed solution it is not enforcing a specific implementation scenario where it is enabling the privacy protection mechanisms as a base for many computational services such as the scheduling, brokering and many other applications. In this work, we are taking the broker as example to evaluate and validate the practicality behind the proposed privacy protection management framework.

Applying the PPF at the computation platform level will improve two main aspects. First of all, the privacy-based platform will maintain the communication aspect where it will carry all the coordination duty with a privacy protection base. As such, the coordination gives a new dimension to communicating where the participant entities are not required to know of each other to accomplish their goal while their privacy is maintained. This will relieve the participant entities from the burden of coordination concerns. Thus, the entities are left with more space and time for other computational activities to improve their profitability and gain a competitive advantage. Injecting the PPF as an essential computational aspect level of the platform will govern the privacy protection based on the requester entity decision that has been taken at the entity level based on the requester entity's privacy property after evaluating information categorization and its exposure boundary that has been identified from the proposed information categorization engine at the entity level. The platform introduces the released shared form of information the privacy protection mechanism, before it establishes the interaction with the registered potential provider. Privacy protection mechanism such as Differential Privacy protection.

The second phase as it is shown in Figure 12: Privacy protection based computational platform is the direct interaction of the requester $e_r$ with the potential service provider $e_p$. At this level there is no intervention of the platform once the potential provider meets all the privacy protection constrains that has been introduced at the platform level. However,

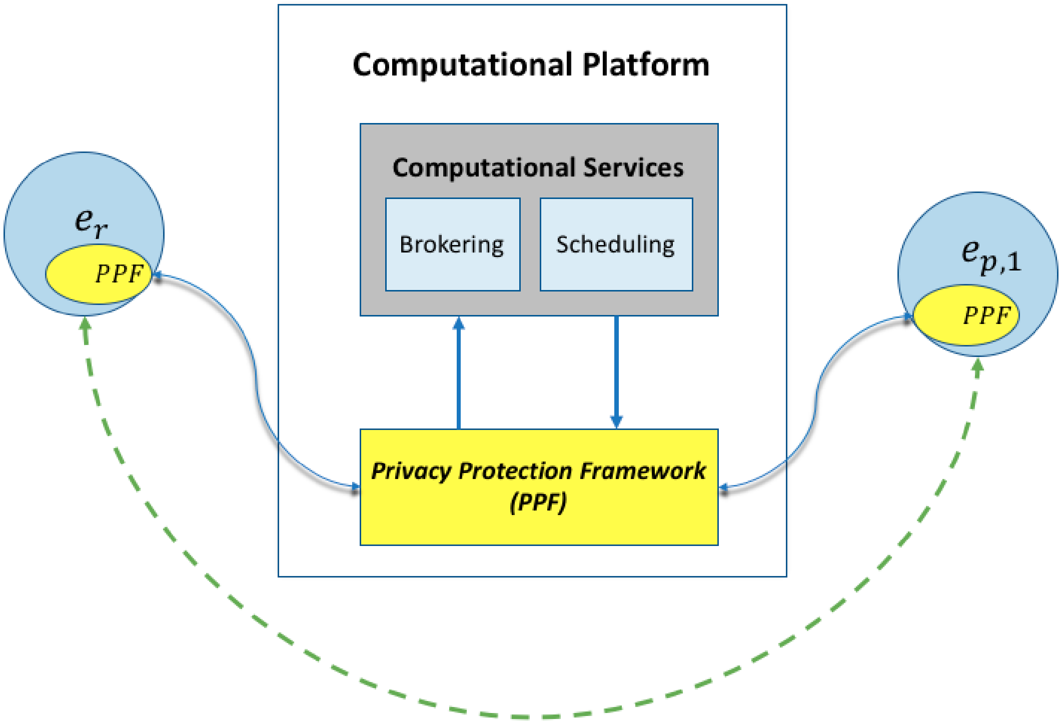


**Figure 12: Privacy protection based computational platform**

the PPF will extend the structure of the entity as well in a way that the participant entities will partially handle the PPF, the privacy protection engine will be carried at the entity level to enable them to measure the sensitivity of their information and set their exposure boundary of the released information in order for the requester $e_r$ entity to make a decision to proceed forward with the interaction.

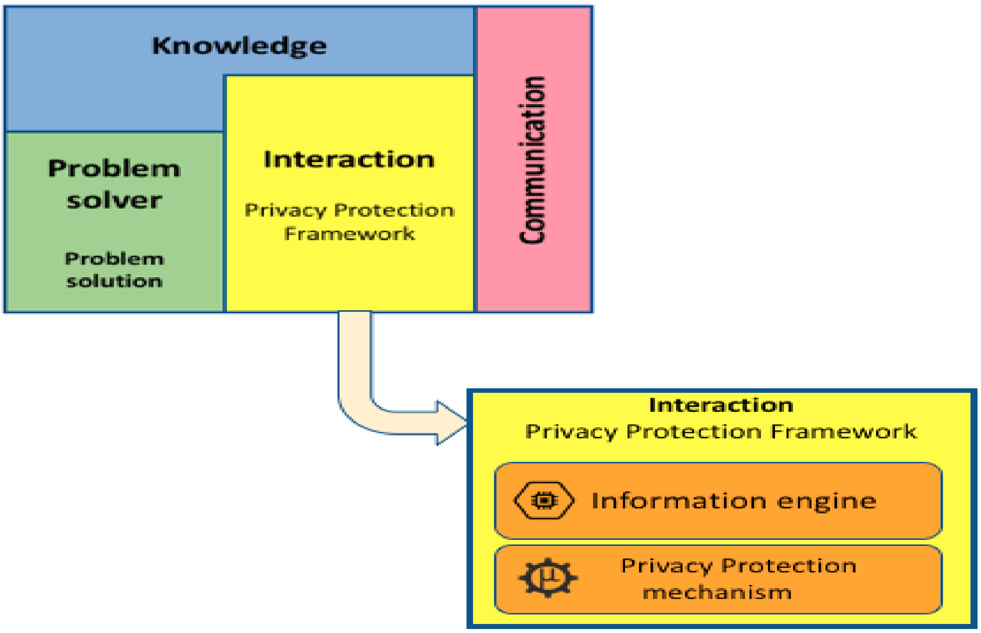


**Figure 13: Privacy Protection Aware Entity**

## 5.5 Summary

The proposed solution is a generic practical model, of the privacy protection framework at the computational level and can address the privacy protection interaction between the participant entities in the environment. Capturing privacy as a computation concept necessitates incorporating the privacy protection within the computation the entity at interaction level. The computation entity in the CDS environment requires resolving interdependency problems through interaction. Treat the privacy concern at the computation level will capture the forms of interactions that have the potential to result in privacy violations. The proposed solution has practically reduced the privacy protection concerns among the participant entities in the CDS environment.

# Chapter 6

# 6 Privacy Protection Platform in CDS Model: Application Scenarios

Many practical applications have been effectively modeled as CDS environments. They are involved within various information system domains. Internet of Things (IoT) is one example that can be effectively modeled as CDS where numerous services, information sources, devices, and sensors are involved. Carrying on with this direction, a Smart-Space is a research initiative at our innovation research lab, through which several studies, analyses and investigations of several critical research issues have been conducted where the privacy concerns and protection in open environments is at the top of the list of our research priority at the lab. In this chapter, we elaborate on the practicality aspect behind the implementation of the proposed privacy protection management framework through utilizing the proposed privacy protection-based platform.

## 6.1 Smart Space Project

The Smart Space project is implemented as an IoT environment in CDS that utilizes a computation integration platform, for which the proposed practical privacy protection framework is partially embedded in the computational platform as a base of interaction for any of the participant smart objects that are looking for a service or providing a service. This will convert the platform to a privacy aware computational platform. Within this environment entities are modeled as Smart Objects (SO) that are managed at the Smart Object Platform (SoP). Services in this environment utilize the existing resources in the space and deliver solutions to applications and services through the interaction. The proposed platform introduces a set of services, such as a brokering layer, to provide functionalities to integrate the resources of the smart space environment including data, services, clouds and events. The proposed privacy protection framework has been introduced through the extension of the CIR-Agent architecture. In order to adopt the proposed framework at the Smart Object (SO) architecture in the smart space need to be mapped to CIR-Agent architecture in away the framework can be adequately implemented.

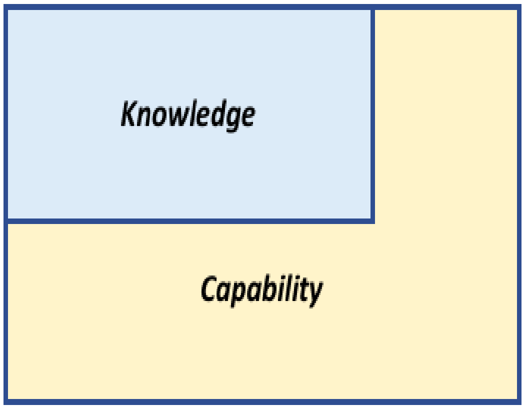


**Figure 14: CIR- Smart Object Logical**

Each of the SOs is composed of knowledge and capability. The main elements of any of the SOs are intelligence, decision and behavior; in this work, we are essentially dealing with the behavior part where the interaction part exists. By mapping between the SO and the CIR-agent:

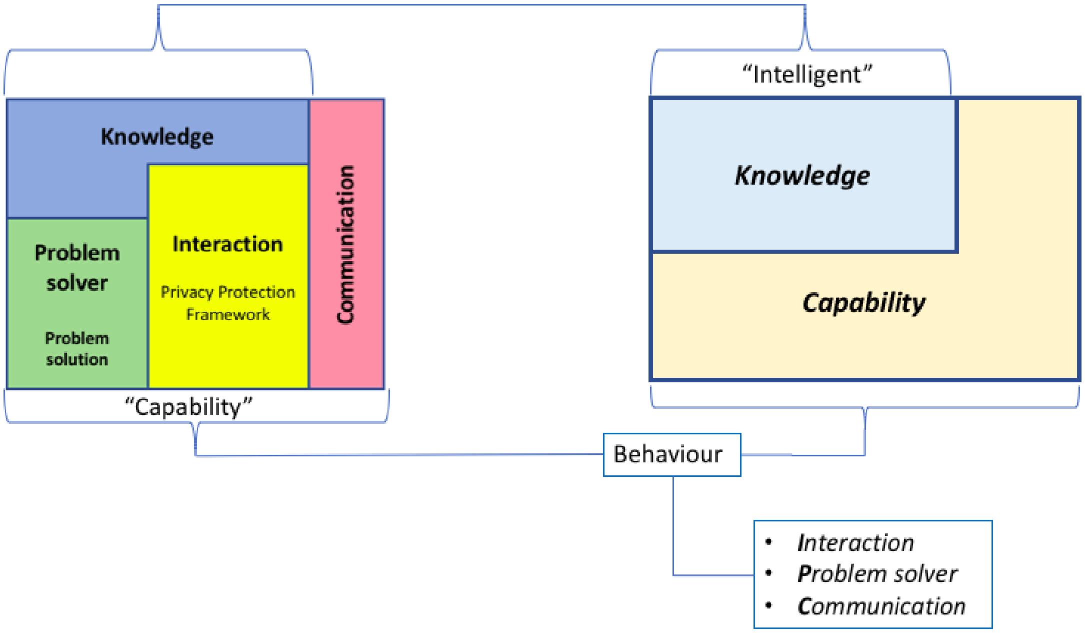


**Figure 15: Mapping the Smart Object to CIR-Agent**

Due to the interdependency problem among smart objects, they require the coordination of their activities using interactions [32], [94]. In the message-based form of interactions, smart objects autonomously interact and exchange information, which leads to privacy concerns. In CDS, solutions are accomplished through the participation of several SOs where each has only one part of the solution. This positions CDS as a computation platform in which the computation occurs in entities' interactions. This entails that privacy challenges in CDS are the concerns associated with the computation happening at the interaction level. This concern can be captured at two levels of privacy-based extension, at the SO "entity" level and at the computation platform as well.

Interaction at the smart object is carried out by the interaction device that has two main components, which are assignment part "Interaction Protocol" and the "Interaction Mechanism". The interaction device is responsible for managing the interaction and the flow of information "into" and "out of" the smart object. Applying the privacy protection management framework at the SO level will reduce the interaction to only SOs who can meet the privacy property of the information owner, then the privacy is considered. By applying the framework principles and giving the exposure boundaries, the sensitive information can be captured. Also, the privacy protection management framework will be responsible for identifying the concern points of the protocol and providing an adequate privacy protection that can turn the interaction protocol to a privacy-based interaction protocol. Utilizing the proposed privacy models and privacy protection management framework as an analytical tool enables identifying the privacy concerns related to the interaction protocol and equipping it with the necessary privacy protection operations.

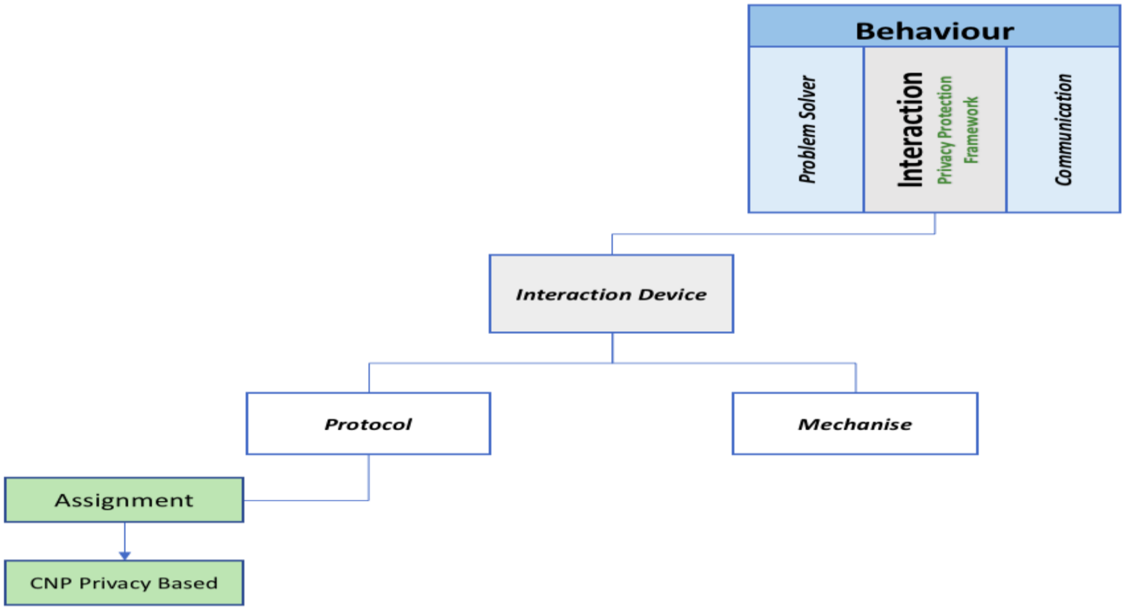


**Figure 16: Smart object privacy-based interaction device**

The other level of the privacy protection implantation at the platform level occurs when the participant $SOs$ are registered with the platform in order to be mapped to the capable potential contractor in the environment. The platform is positioned as a base for any computational service, in which those computational services will be responsible for managing the coordination among the participant $SOs$. Extending the computational platform with privacy protection will set the privacy as an essential aspect for any interaction between the requester $SO$ and the computational service and between the potential participant provider $SOs$ in an open distributed environment to deliver services.

In the Smart Space project, we have adopted the DEXIT computational platform, which is an Integrated Channel Engagement (ICE) platform, that provides and supports all kinds of engagements as a cloud base [26]. The interaction in the platform among the participant entities occurs through the smart object platform (SOP). Any domain can be modeled and managed through the business concept platform (BCP). According to the environment settings, the privacy protection framework (PPF) can be adequately applied as a computational aspect at the interaction part of the smart object beside the interaction level of the platform as well, which is the SOP.

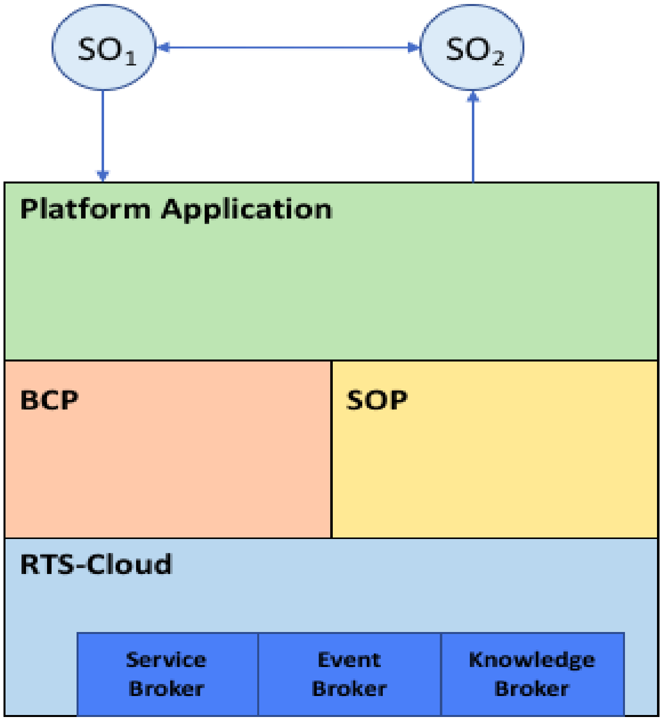


**Figure 17: Computational Engagement Platform "DEXIT"**

## 6.2 Privacy concerns and protection in Smart Space

The motivation behind the smart space is to create an Internet of Things (IoT) environment where a variety of autonomous smart objects (i.e., things) are networked to utilize and provide services to the environment [7]. The participant smart objects, “things”, will be able to communicate and interact with each other through the interaction to collect and exchange data over a network with minimal human intervention [2]. Furthermore, the future growth of IoT based applications is foreseen to be tremendous [12]. The incorporation of social networks and ubiquitous computing technologies in IoT can easily collect data about our personal characteristics and behaviors. For individuals and groups of people, there are many advantages of interacting seamlessly with the environment incorporating IoT into their lives [75], [48], [30]. The comfort experienced via innovative technologies in IoT is at the expense of privacy [68], [10], where the privacy of individuals can be compromised in IoT. As such, a massive amount of personal information is observed without informing users, let alone asking for their permission [10]. Consequently, the more engagements involved among individuals with IoT based applications and their enabling technologies, the more privacy concerns will arise [79], [80], [81].

As the smart space inherits the characteristics of IoT, the privacy challenge within this environment will endure. Since the IoT is modeled as a CDS, privacy concerns and protection occur during the interaction among smart objects that do exist in the space.

### 6.2.1Privacy Concern Scenarios

In the smart space, Smart Objects have their own goals that they pursue. Those $SOs$ need to interact and share their capabilities in order to achieve the required goals. The goal information $I^{gol}$ needs to be shared with the capable $SOs$ who can achieve the requested goal. The shared $I^{gol}$ with a specific $SO$ might be considered sensitive information if it has been revealed to another set of $SOs$ that might introduce operations to extract implicitly sensitive information from explicitly shared information. In this case, the information needs to be managed and the potential participant $SOs$ need to be categorized based on their relation with the shared information $I^{int}$ in relation with the $SOs$ before it is shared. Due to the exchange of information in interactions smart space, privacy becomes a concern for all the participants.

In the smart space project, we have applied the education domain which is MyPLS (my Personal Learning Space), which is mainly about enabling Active learning for E-learning. MyPLS has a set of features that enable students and learners to create and manage their learning space. Each of the participant can contact and establish conversations and/or chatting about learning topics relevant to the group's interest.

There are a set of participants learner smart objects $(SO_i, \dots, SO_t, \dots, SO_N)$ registered in the platform, each of which $SO$ has an interest and they need to get assistance in a specific topic $I^t$, where there is a learner $SO_{L1}$ that requires the topic resources $I^t$. The interest in the required topic has been shared with everyone who has the same topic of interest $(SO_i, \dots, SO_t, \dots, SO_N)$. Executing operations on the shared interest $I^t$ can extract a new form of information that the $I^t$ owner is not willing to reveal and might return with a negative impact on the $SO_{L1}$, such as disseminating $I^t$ of the $SO_{L1}$ to another $SO_x$ that does not have the same topic of interest is raising the flag of privacy concern about $\mathrm{SO}_{\mathrm{L1}}$ privacy by manipulating the information about the interest and extracting an implicit form of information that the $SO_{L1}$ explicitly shared. This scenario is one of the forms of privacy concerns, "Discrimination Privacy Concern"[88] , [89]. In such an environment, it is essential that entities receive privacy protection while interacting with each other in finding a mutual topic of interest.

### 6.2.2 Privacy Protection Platform based.

Given the earlier analysis of the proposed privacy protection framework implementation at the computation level, the framework elements have been practically determined as a computational concept that is partially applied at two levels; the entity level and platform level, that will consider the privacy protection at all of the computational levels. This is illustrated through the extension of the $SO$ and extension on the platform as privacy based.

Introducing the first part of the solution by injecting the part of privacy protection management framework at interaction level will allow smart objects to handle the decision-making process. In a way any $SO$ can measure the chance of a privacy concern by measuring the risk of interaction, which is directly related with the requester $SO$ information utility in relation with the potential $SOs$. Therefore, it becomes a multi-objective problem to allocate proper protection operations with an adequate level of PPL serving the expected utility and the requested task.

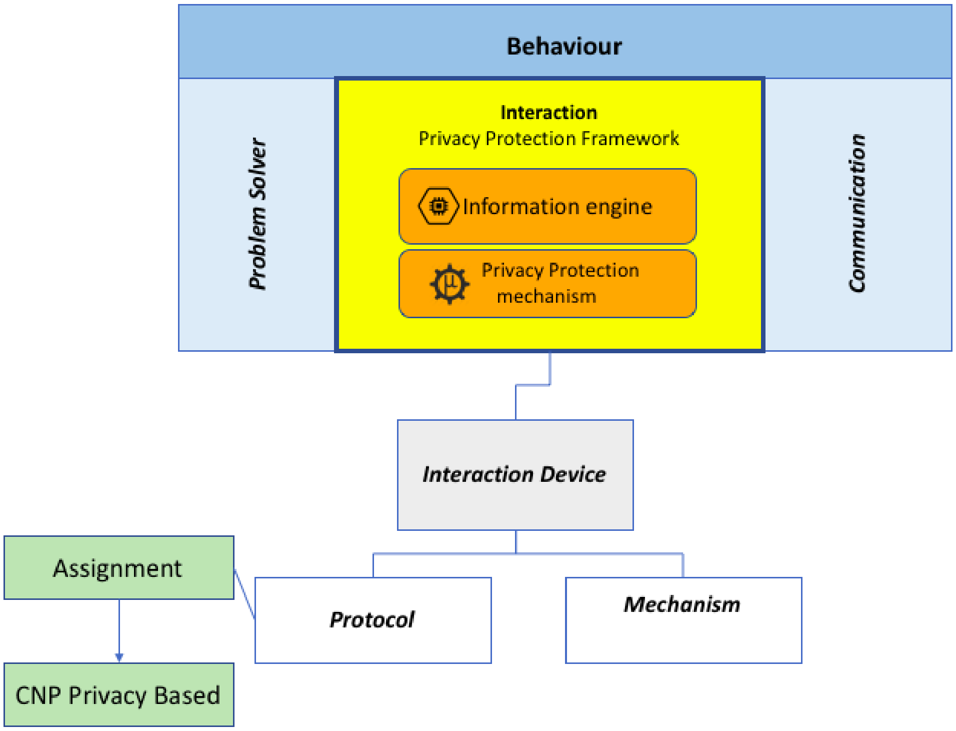


**Figure 18 Smart Object Privacy Protection Aware**

Capturing the proposed solution at the entity level will allow identifying privacy concerns at the interaction protocol and evaluates the messages and sequences of the interaction protocol and provides adequate protection operations within the interaction protocol that result in a privacy-based interaction protocol. The extended privacy-based interaction protocol that is generated by applying the privacy protection management framework can sufficiently provide privacy protection in situations where the knowledge in the CDS environment is incomplete.

The second level of the proposed solution is the computation privacy protection platform base. The proposed platform will carry the burden of the coordination. The coordination is maintained under the privacy protection propriety of the privacy protection framework.

Participant $SOs$ do not need to be concerned with how the interaction and the coordination are performed with potential $SOs$, in which the platform will manage capability-based coordination while the assignment interaction protocol manages the brokering capability of various $SOs$.

Extending $SOs$ with privacy protection is possible by injecting the proposed framework as a computational aspect after applying the other part of the framework at the platform. Having such an implementation will ensure that any interaction and solution will be based on the privacy protection as a constraint. Also, the platform structure is extended along with the other parts of the privacy protection framework. Under this implementation, any of the participant entities are interacting through the privacy protection-based platform after assessing its privacy protection at the $OSs$ level first and then proceeding to the interaction with the privacy protection part at the computational platform.

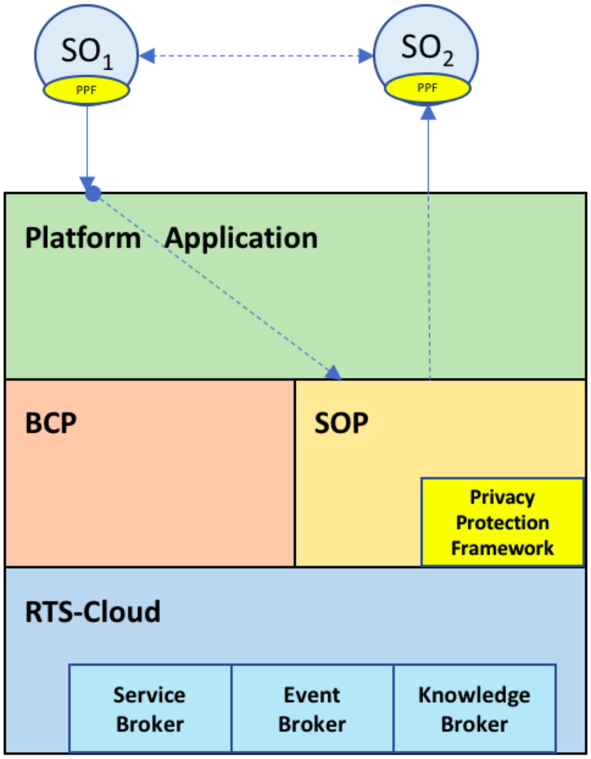


**Figure 19: Computational Privacy Based Engagement Platform**

## 6.3 Summary

The smart space project is defined as including a diverse set of entities to form an IoT environment and is modeled as a CDS. “Entities” in this smart space are modeled as smart objects ($SOs$). Because of the increased involvement of people and their devices in IoT applications, privacy has become a more complex challenge. Hence, we have applied privacy protection-based smart objects that do exist on a privacy protection-based environment in a smart space.

As smart objects in the open environments are autonomous and self-interested, it is assumed that all entities will respect the privacy of each other. Applying the proposed privacy protection framework (PPF) on the participant $SOs$ will transfer any $SOs$ to privacy protection aware so as to deliver any solutions utilizing privacy protection-based platforms that carry PPF as a base as well. This will provide the available solutions restricted only to those that can accept the privacy constraints. Therefore, privacy becomes a quality factor of any of the requested solutions.

# Chapter 7

# 7 Privacy Protection-Based Implementation

The focus in this implementation is to provide a functional specification of CDS (Cooperative Distributed System). In our implementation, applications and services are connected and integrated through a computational platform. In which, it facilitates the cooperation, interaction and integration among participant Smart Object $(SOs)$. Applying the proposed privacy protection management framework will provide a reasonable privacy protection as a computational concept.

Technically, we have chosen DEX computational platform, where all of the computation services, such as web service and DB to be deployed at DEX platform. Also, all the participant $SOs$ will interact with each other utilizing the platform. By introducing the proposed privacy protection management framework partially at the $SO$ and at the computational platform, privacy concerns will be handled from following perspectives:

- Sensitive information categorization.
- Exposure boundary identification.
- Privacy protection operation.

## 7.1 Experimental setup

This section describes the experimental setup:

### 7.1.1 Architecture Level

The main two rolls in our solutions that in our implementation that we are focusing on are the Service Requesters and Service Providers, whom are interact and communicate through computational platform utilizing the computation service such as brokering manager layer.

1) **Service requester SO:** Requesters interact with brokering layer through the privacy protection management framework-based platform. During the interaction

process, service requester will have the capability to make decision among multiple providers' proposals. After assessing the privacy protection requirement for each of the participants providers according to the service requester.

2) **Service providers SO:** Providers have no direct interaction with the service requester. At the first stage, the interaction in the beginning will interact through the privacy protection-based platform. Second stage, direct interaction after the privacy protection has been evaluated for each provider at two levels: the entity level evolution and the platform level.

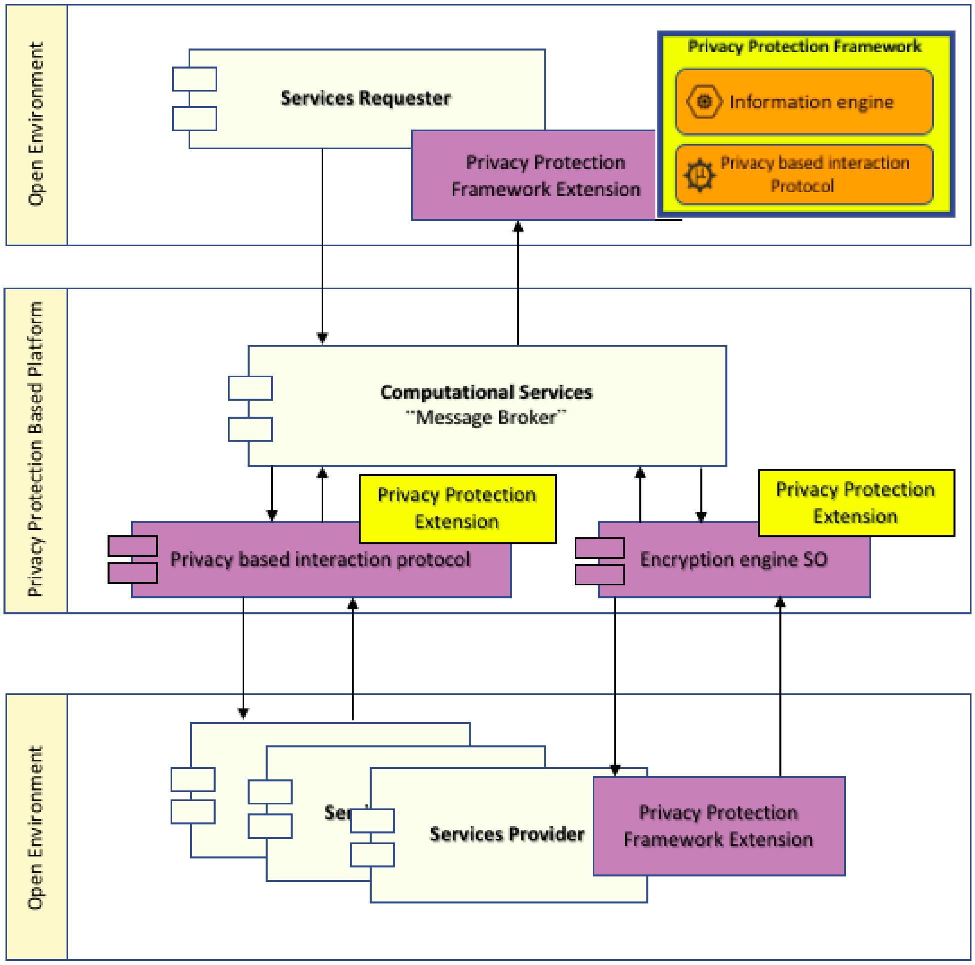

Open Environment
Services Requester
Privacy Protection Framework
Information engine
Privacy based interaction Protocol
Privacy Protection Framework Extension
Privacy Protection Based Platform
Computational Services
"Message Broker"
Privacy Protection Extension
Privacy based interaction protocol
Privacy Protection Extension
Encryption engine SO
Open Environment
Ser
Services Provider
Privacy Protection Framework Extension

**Figure 20: System Architecture**

### 7.1.2 Deployment Level

1) All the participant “requester” will be registered in DEX’ service broker. Requestors in will only know the DEX’s host as the privacy protection-based platform. In which, it hosts the broking layer as a computation service.

2) All potential providers modeled as smart object ($SO$) in DEX. The providers SOs will receive a broadcasted task from one of the computation services that exist on the computational platform.

3) All the of capable potential providers will response to the required task message. The responded message includes the key identifier of each provider.

4) Responses will be collected by one of the computation services, ex. Broker, through the privacy protection element of the framework at the platform. The collected responses will be forwarded to the decision making SO cooperative with initial requester to make a decision based on requester privacy preference.

5) In Heroku platform, another smart object to support encryption engine services will be implemented and deployed.

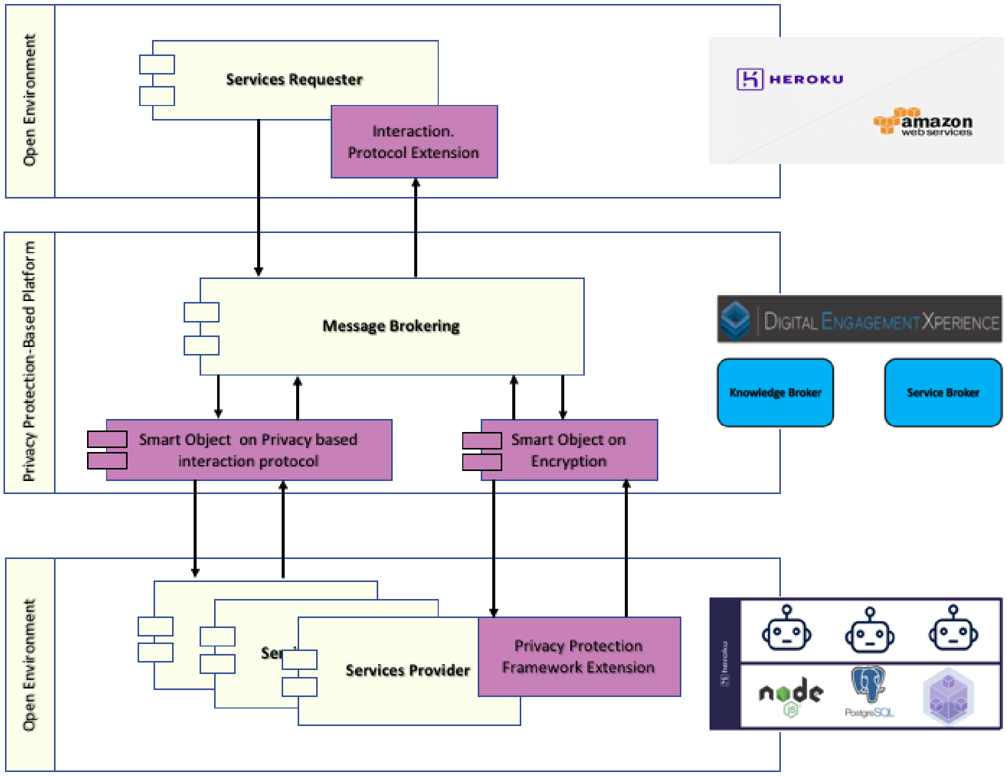

Open Environment
Services Requester
Interaction. Protocol Extension
HEROKU
amazon web services
Privacy Protection-Based Platform
Message Brokering
DIGITAL ENGAGEMENT XPERIENCE
Knowledge Broker
Service Broker
Smart Object on Privacy based interaction protocol
Smart Object on Encryption
Open Environment
Ser
Services Provider
Privacy Protection Framework Extension
heroku
node
PostgreSQL

**Figure 21: Deployment Architecture**

### 7.1.3 Design Principle on Privacy Concerns

1) Build a computational privacy layer to deal with the request, response and negotiation process, which can avoid direct interaction between the participant SOs. This layer will lower the risk of information leaking and privacy concern.
2) All potential providers will register their service in brokering layer, which makes the real request path and services are anonymous.
3) All potential providers are hiding their capability and will check the capability based on the requested task.
4) During the request inquiring process, the requester explicit information has to be reduced as possible as it can be. Normally, the 'task ID' is the explicit form of information that is shared.
5) During the interaction, the task value will be encrypted; only the requester has the authority to decrypt the task value for the potential winner provider by sharing the encryption key.
6) All the capable selected providers will contact the Privacy Protection Layer, which is specifically the Encryption SO, to get the encrypted task value. Then forward it's service id to the computational service, ex. Message Broker computational service.

The Brokering SO collects all bidding encrypted information and transfer to requester SO. Requester SO need to contact Encryption engine at the platform to decrypt the task and select the winner provider. Afterwards, winner provider interacts directly with the requester SO to execute the task without the intervention of the platform.

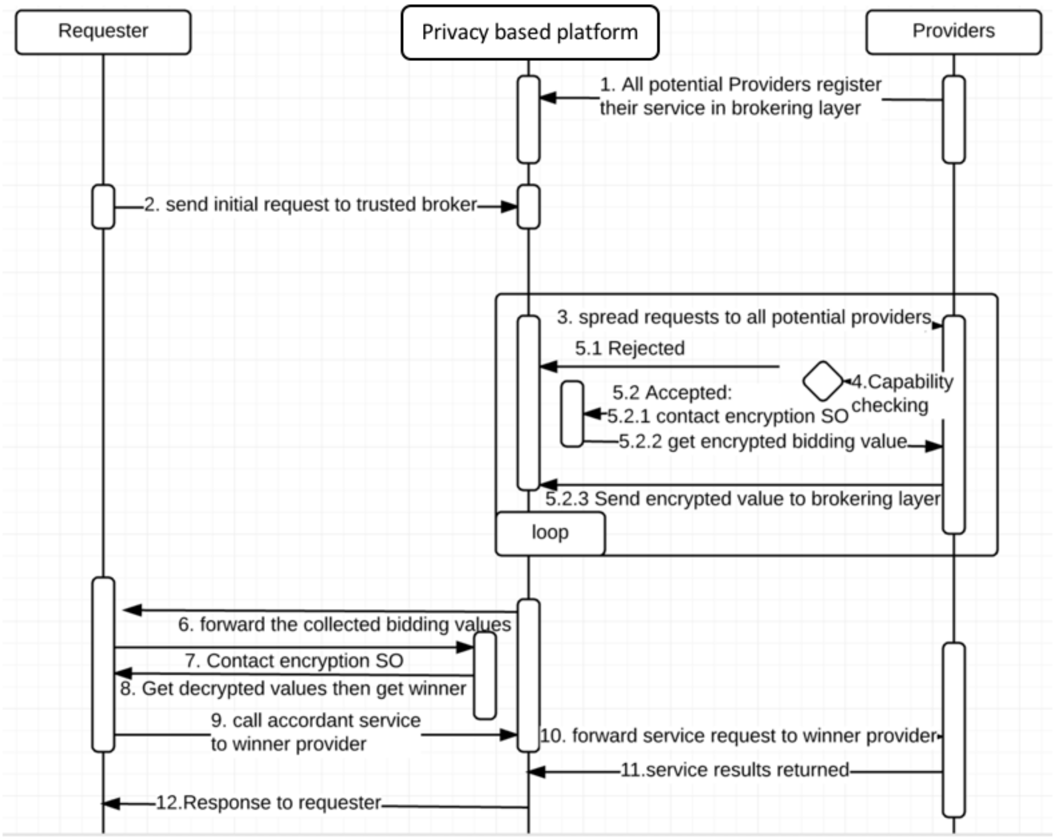

Requester
Privacy based platform
Providers
1. All potential Providers register their service in brokering layer
2. send initial request to trusted broker
3. spread requests to all potential providers
5.1 Rejected
4.Capability checking
5.2 Accepted:
5.2.1 contact encryption SO
5.2.2 get encrypted bidding value
5.2.3 Send encrypted value to brokering layer
loop
6. forward the collected bidding values
7. Contact encryption SO
8. Get decrypted values then get winner
9. call accordant service to winner provider
10. forward service request to winner provider
11.service results returned
12.Response to requester

**Figure 22: Privacy Protection-Based Interaction Protocol**

## 7.2 Detailed Design and Implementation

Based on the previous designed scenario, the requester in Salesforce will send a ‘TaskRequest’ to ‘provider smart object’. The ‘provider smart’ will evaluate the bid details and set their capability, synced back with Salesforce in real-time.

## 1. Service registration in DEX platform

Request the TOKEN:

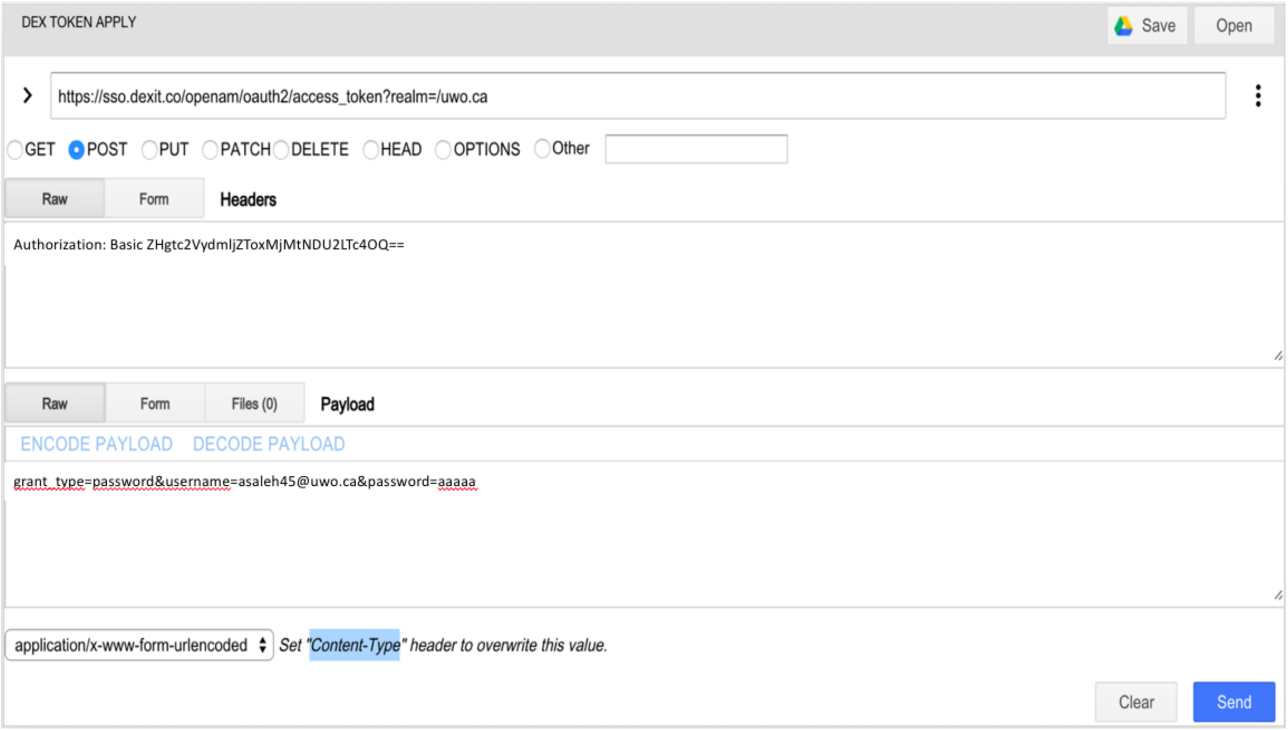
URL : https://sso.dexit.co/openam/oauth2/access_token?realm=/uwo.ca

Method: POST

Headers: Authorization: Basic ZHgtc2VydmljZToxMjMtNDU2LTc4OQ==

Content-Type: application/x-www.form-urlencoded

Body: grant type=password&username=asaleh45@uwo.ca&password=aaaaa



https://sso.dexit.co/openam/oauth2/access_token?realm=/uwo.ca

○GET ●POST ○PUT ○PATCH ○DELETE ○HEAD ○OPTIONS ○Other

Authorization: Basic ZHgtc2VydmljZToxMjMtNDU2LTc4OQ==

grant_type=password&username=asaleh45@uwo.ca&password=aaaaa

application/x-www-form-urlencoded *Set "Content-Type" header to overwrite this value.*

**Figure 23: Service registration at the platform**

## 1.1 DEX Service Broker Registration:

URL : http://sb-a1.herokuapp.com/services

Method: POST

Headers: Authorization: Bearer 7cd44fa9-2414-4b74-8c50-0ab15be14fa2

Content-Type:application/json

Body : {"service_name": " Project-SO1-PB_SO",

"type":"restful",

"description":"",

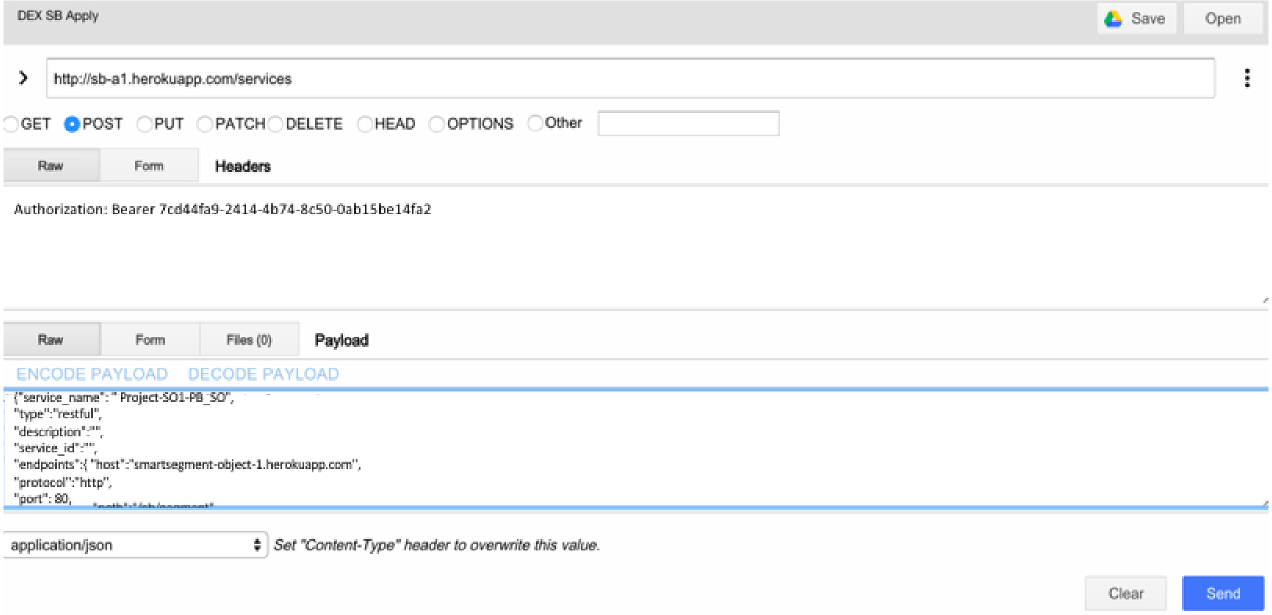
"service_id":"",

"endpoints":{ "host":"smartsegment-object-1.herokuapp.com",

"protocol":"http",

"port": 80,

"path":"/sb/segment" }



http://sb-a1.herokuapp.com/services

○ GET ● POST ○ PUT ○ PATCH ○ DELETE ○ HEAD ○ OPTIONS ○ Other

Authorization: Bearer 7cd44fa9-2414-4b74-8c50-0ab15be14fa2

```
{"service_name":" Project-SO1-PB_SO",
"type":"restful",
"description":"",
"service_id":"",
"endpoints":{ "host":"smartsegment-object-1.herokuapp.com",
"protocol":"http",
"port": 80,
        "path":"/sb/segment"
```

application/json *Set "Content-Type" header to overwrite this value.*

**Figure 24: Service broker registration**

### 1.2 DEX Service Execution

1. Add service id in URL
2. Put TOKEN in headers

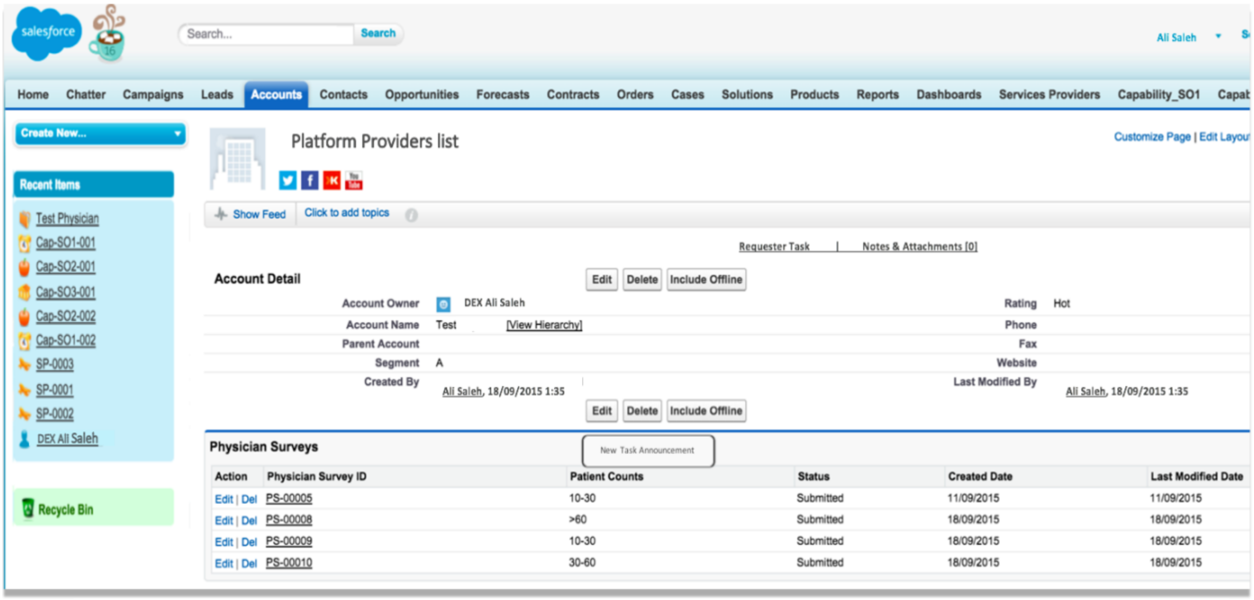
URL : http://sb-a1.herokuapp.com/execution/707844e7-33ba-43fc-bd57-75d9fed96239

Method: POST

Headers: Authorization: Bearer e8510aca-6e53-41ee-8735-f81c3464f256

## 2. Requester smart object: Salesfoce.com + decision-making SO in Heroku

- All the requesters start resaving the task request after collecting the (TaskRequest) announcement, and they response back with can send the segment update request to start the interaction.
- The service requester will revise the service description from Brokering layer has been registered in DEX and service id is saved in salesforce side and get ready to be called anytime.



Platform Providers list

Account Detail

| | | | |
|---|---|---|---|
| Account Owner | DEX Ali Saleh | Rating | Hot |
| Account Name | Test [View Hierarchy] | Phone | |
| Parent Account | | Fax | |
| Segment | A | Website | |
| Created By | Ali Saleh, 18/09/2015 1:35 | Last Modified By | Ali Saleh, 18/09/2015 1:35 |

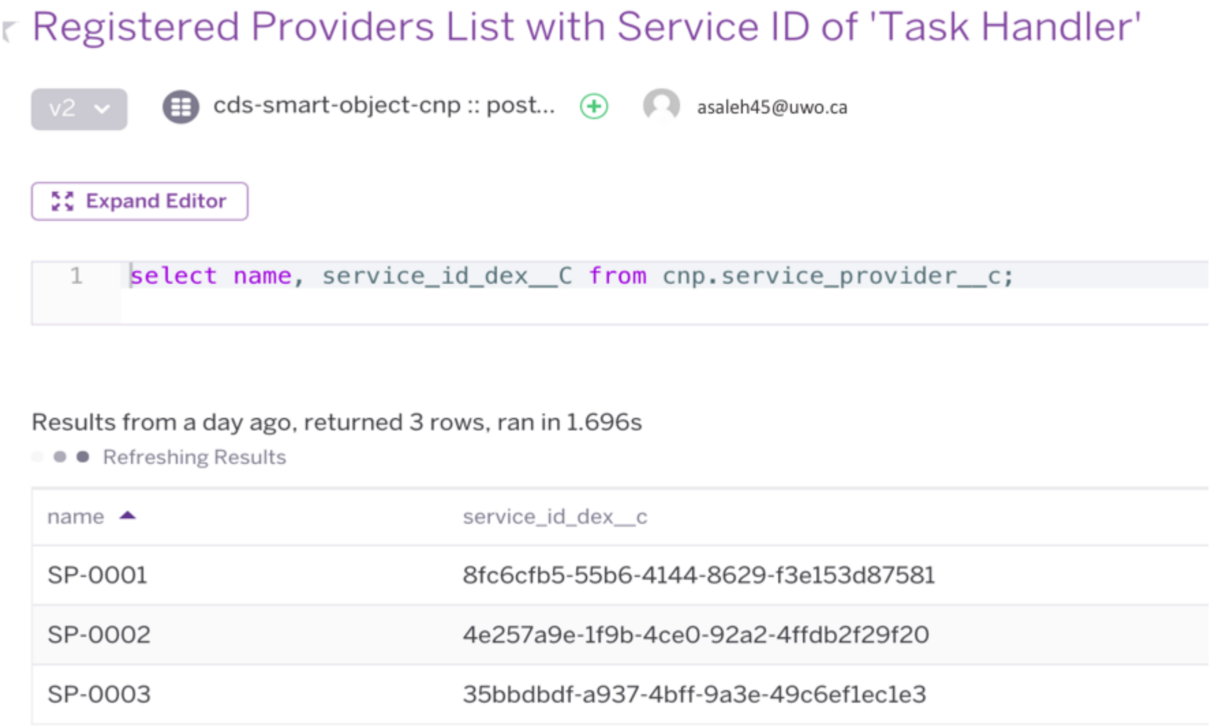
Physician Surveys

| Action | Physician Survey ID | Patient Counts | Status | Created Date | Last Modified Date |
|---|---|---|---|---|---|
| Edit \| Del | PS-00005 | 10-30 | Submitted | 11/09/2015 | 11/09/2015 |
| Edit \| Del | PS-00008 | >60 | Submitted | 18/09/2015 | 18/09/2015 |
| Edit \| Del | PS-00009 | 10-30 | Submitted | 18/09/2015 | 18/09/2015 |
| Edit \| Del | PS-00010 | 30-60 | Submitted | 18/09/2015 | 18/09/2015 |

**Figure 25: Requester Smart Object**

## 3. Brokering layer: DEX platform + CNP Smart Object in Heroku

All service providers' entry services will be registered in DEX and saved in Heroku as a CNP SO's. After they receive the request, the CNP SO will broadcast the request to potential providers with task ID and requester ID.



Registered Providers List with Service ID of 'Task Handler'

```
select name, service_id_dex__C from cnp.service_provider__c;
```

Results from a day ago, returned 3 rows, ran in 1.696s

| name ▲ | service_id_dex__c |
|---|---|
| SP-0001 | 8fc6cfb5-55b6-4144-8629-f3e153d87581 |
| SP-0002 | 4e257a9e-1f9b-4ce0-92a2-4ffdb2f29f20 |
| SP-0003 | 35bbdbdf-a937-4bff-9a3e-49c6ef1ec1e3 |

**Figure 26: Platform Brokering Layer**

Once receiving the bidding values from capable potential providers, the CNP SO will collect the bidding values and accordant service id and forward to requester's decision-making SO.

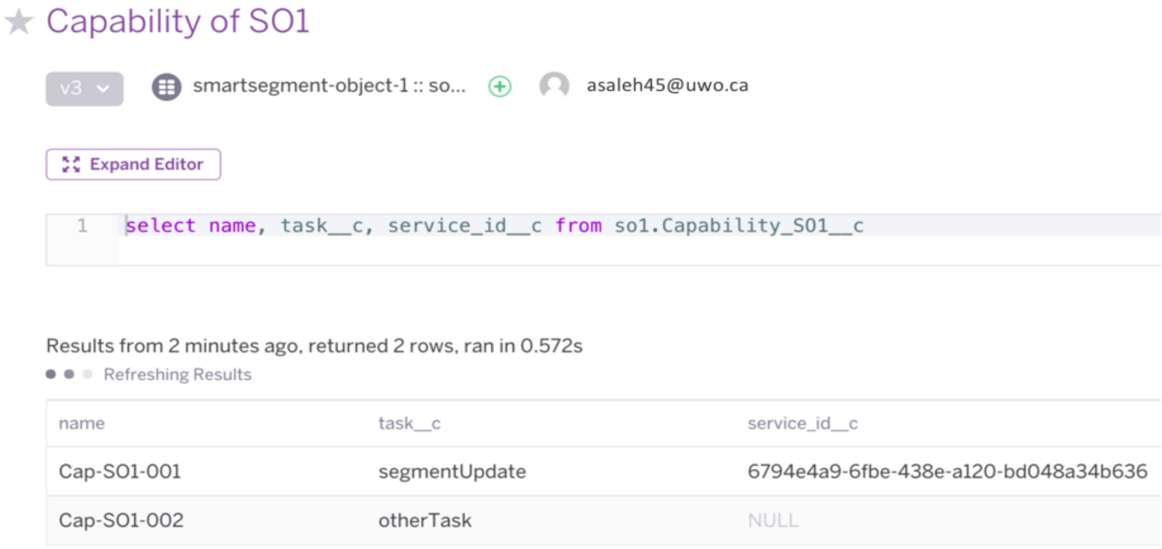
## 4. Decision-making SO with requester

Once receiving the bidding values from brokering layer, the requester's decision-making SO will interact with encryption SO to decrypt the bidding values then select the winner provider with the accordant service ID. Requester will forward its request with winner' service ID to execute the service and get the result.

## 5. Service Providers in Heroku

After receiving the task notice from CNP SO, the provider will check its own capability, if it is capable to solve this task, the encrypted bidding value will be generated through interacting with encryption SO to retrieve the key and register the trusted requester id.

- Capability registered table:



```
select name, task__c, service_id__c from so1.Capability_S01__c
```

Results from 2 minutes ago, returned 2 rows, ran in 0.572s

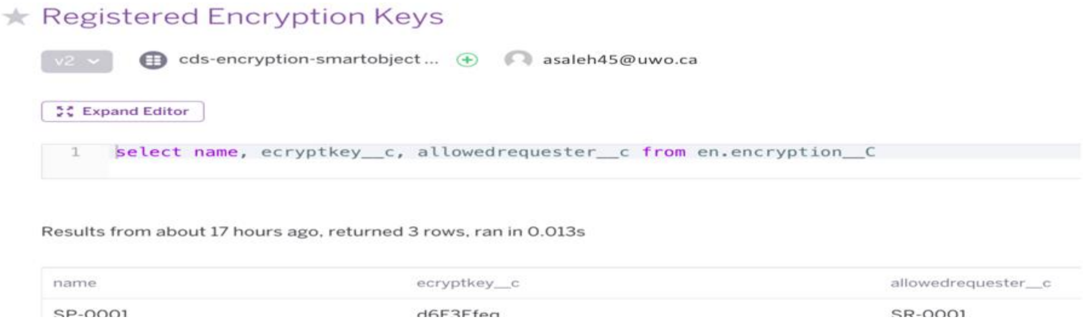
Refreshing Results

| name | task__c | service_id__c |
|---|---|---|
| Cap-S01-001 | segmentUpdate | 6794e4a9-6fbe-438e-a120-bd048a34b636 |
| Cap-S01-002 | otherTask | NULL |

**Figure 27: Capable Potential Provider**

## 6. Smart Object for encryption

In this SO the accordant keys mapping to specific service provider are saved, we can define different encryption algorithm to offer encrypt or decrypt service.



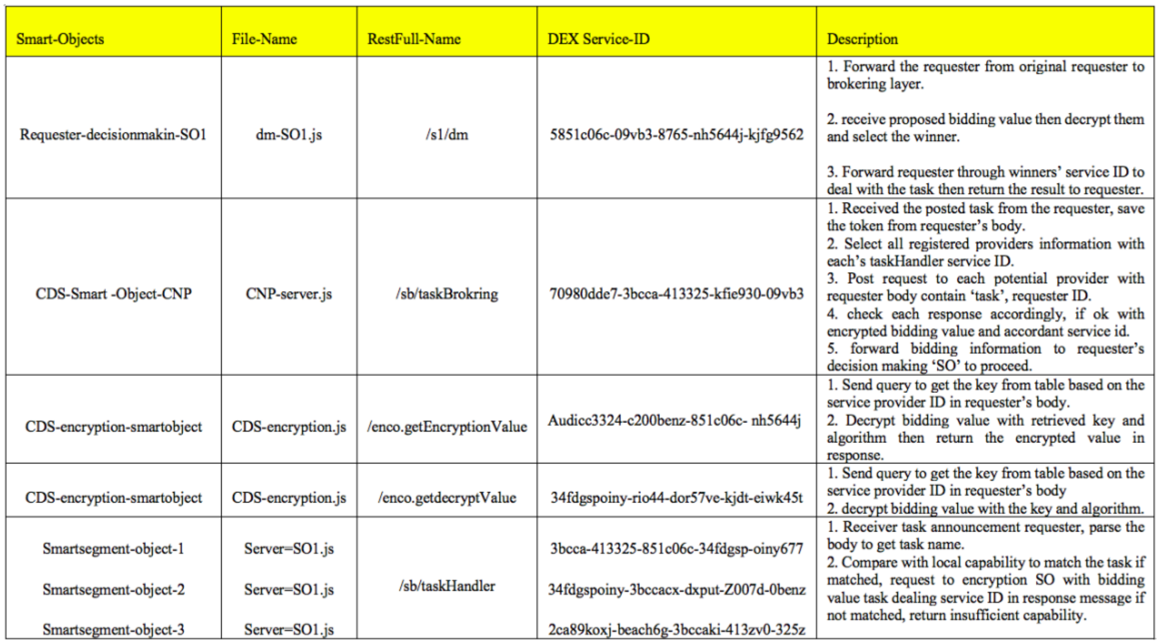
```
select name, ecryptkey__c, allowedrequester__c from en.encryption__C
```

Results from about 17 hours ago, returned 3 rows, ran in 0.013s

| name | ecryptkey__c | allowedrequester__c |
|---|---|---|
| SP-0001 | d6F3Ffeq | SR-0001 |

**Figure 28: Encrypt and Decrypt Service**

## 7. API and Services List in Heroku platform with Node.js.



| Smart-Objects | File-Name | RestFull-Name | DEX Service-ID | Description |
|---|---|---|---|---|
| Requester-decisionmakin-SO1 | dm-SO1.js | /s1/dm | 5851c06c-09vb3-8765-nh5644j-kjfg9562 | 1. Forward the requester from original requester to brokering layer.<br>2. receive proposed bidding value then decrypt them and select the winner.<br>3. Forward requester through winners' service ID to deal with the task then return the result to requester. |
| CDS-Smart -Object-CNP | CNP-server.js | /sb/taskBrokring | 70980dde7-3bcca-413325-kfie930-09vb3 | 1. Received the posted task from the requester, save the token from requester's body.<br>2. Select all registered providers information with each's taskHandler service ID.<br>3. Post request to each potential provider with requester body contain 'task', requester ID.<br>4. check each response accordingly, if ok with encrypted bidding value and accordant service id.<br>5. forward bidding information to requester's decision making 'SO' to proceed. |
| CDS-encryption-smartobject | CDS-encryption.js | /enco.getEncryptionValue | Audicc3324-c200benz-851c06c- nh5644j | 1. Send query to get the key from table based on the service provider ID in requester's body.<br>2. Decrypt bidding value with retrieved key and algorithm then return the encrypted value in response. |
| CDS-encryption-smartobject | CDS-encryption.js | /enco.getdecryptValue | 34fdgspoiny-rio44-dor57ve-kjdt-eiwk45t | 1. Send query to get the key from table based on the service provider ID in requester's body<br>2. decrypt bidding value with the key and algorithm. |
| Smartsegment-object-1<br>Smartsegment-object-2<br>Smartsegment-object-3 | Server=SO1.js<br>Server=SO1.js<br>Server=SO1.js | /sb/taskHandler | 3bcca-413325-851c06c-34fdgsp-oiny677<br>34fdgspoiny-3bccacx-dxput-Z007d-0benz<br>2ca89koxj-beach6g-3bccaki-413zv0-325z | 1. Receiver task announcement requester, parse the body to get task name.<br>2. Compare with local capability to match the task if matched, request to encryption SO with bidding value task dealing service ID in response message if not matched, return insufficient capability. |

**Table 1: API and Services Content List.**

The model can be applied in different 'smart space' domains that is an open environment based and its entities required a cooperation and need to interact with other entities to solve their problem. The architecture is fitting in the agile development without concerning infrastructure, since the applications and database can be deployed in cloud base platform such as Heroku. In such, the integration and scalability with the privacy-based platform would be easier since the framework is introduced as add-ons to any platform.

# Chapter 8

# 8 Conclusion and Future Work

The aim of the research presented in this dissertation is to define a generic practical treatment of “privacy concern” as a computation concept in CDS paradigm that is implemented as practical privacy-aware solution. The formal model of privacy protection is practically introduced as a base for privacy protection management framework for CDS. This has been served at two different levels of privacy protection, which are privacy-aware agent model and privacy-based computational platform for CDS that enables privacy protection at the interaction level. In addition, based on the privacy protection management framework the interaction protocol has been practically delivered as privacy base interaction protocol.

## 8.1 Contributions summary

Entities in distributed systems such as CDS are autonomies and has a level of authority to interact and exchange information during the interaction to achieve individual or collective goals [32], [94]. Due to interdependency Information exchange through the interaction of autonomous and self-interested entities. Thus, this raise the privacy concern that can occur behind such exchange of information and the operations that might be executed on it [71], [56]. This work has contributed in several aspects of these areas, which is shared with privacy protection in information management, uncertainty level of privacy protection identification, privacy concepts and practical information categorization within multi-agent systems and practical privacy protection management framework implementation at computational level.

### 8.1.1Challenge and Contributions

Despite the rapidly growing development of applications, user’s privacy is becoming a critical issue. Thus, distributed systems architects, developers and administrators are facing the challenge of securing user’s privacy as well as the services they might access. Privacy, by nature is a concept that is defined with many denotations, which could be interpreted differently in various contexts. Understanding privacy as a concept that can be applied in contexts such as CDS requires formal analysis of settings in which privacy is not negligible. Our major contribution in this work is to introduce a practical privacy-aware computation in open Cooperative Distributed Systems that addresses and manages privacy at the interaction level. This has been introduced at three levels: First of all, verifying the legitimacy of the achieved solution after applying the privacy as constrain. Secondly, impose privacy protection in the solution as a computation concept. To resolve privacy concerns in CDS, it is essential that privacy is modelled in a context that is adequate for CDS environments. Third, assess the practicality of the proposed solution of intruding it at the entity level and at the platform level. Modeling privacy in information management context can be categorized as information collection, information processing and information dissemination through which it can adequately be applied in CDS environments. Due to dynamicity of the open environments, architectural-based approaches are more desirable for CDS environments. For which, in this work we pursue the computation view on privacy protection solution within the information management context and adopt the architectural-based solution approaches by applying the model at the interaction level at the entity level and at the platform level.

In this work a practical implementation of the formal model for privacy concern in an information management context is presented. Where it has dealt with the privacy concern as a critical issue in decentralized environments since there is no centralized control and knowledge in the open environment, where both of them are distributed among autonomous, self-interested entities and they need to adopt message-based interactions through which information is shared. “Sharing” is a supervised process by entities, and as such depending on the receiver of the information, the entity does not share the information that is classified as *sensitive*. Privacy concern in this work molded as sensitive information can be sensitive in relation to an entity and become non-sensitive in relation to another. That will identify the state exposure boundary for which information that can demonstrate the sensitivity of information with other existed participant entities in the space. Due to the incomplete knowledge of entities in CDS, we addressed the uncertainty level of privacy protection in quasi mechanisms, a probabilistic model is utilized that reflects conditional probability of privacy protection given the information that exists at the entity. This concept is addressed as Privacy Protection Level (PPL).

Within this work, we have applied the privacy protection management framework partially at the computation level by expanding the structure of the entity and elevating and elevate the rest at the computational platform to include privacy protection management that adheres to the privacy-based interaction protocol. this demonstrate that legitimate acceptable solutions at the computation require the inclusion of privacy resolution in-addition to problem solving and coordination.

## 8.2 Future Work

The contributions scoop in this work were molding the privacy concern, categorize information in relation with potential participant entities, identifying an information exposure boundary in context of open environment, practicality analysis of the proposed privacy protection management framework under the focus of feasibility and efficiency, and providing a practical implementation of the privacy protection management framework to introduce a privacy protection aware entity and privacy protection base platform. This work can be expanded within the area of economic-based privacy model and optimization of privacy protection management. Economic mechanisms are adequate models for managing interactions in decentralized systems. There are many research works attempt to adopt the economic mechanisms to solve complex decision problems in CDS [87], [96]. Modeling privacy using economic based approaches can provide alternatives in which entities willingly consider the privacy of others. Because entities are economically rational, the expected outcome is the elimination of the chance of executing operation that transforms non-sensitive information into sensitive. Therefore, the solution to privacy can behave as perfect protection mechanisms [12][75][48][30].

# References

[1]. A. Hongwei. (d, k)-Anonymity for Social Networks Publication against Neighborhood Attacks. (2013). *Journal of Convergence Information Technology*, 8(2), pp.59-67.

[2]. A.Juels. Targeted advertising ... and privacy too. Presented at Proceedings of the 2001 Conference on Topics in Cryptology: The Cryptographer's Track at RSA. 2001, Available: http://dl.acm.org/citation.cfm?id=646139.680791.

[3]. A.Petcu and B. Faltings. DPOP: A scalable method for multiagent constraint optimization. Presented at IJCAI 05. 2005, .

[4]. A.Samani, H. H. Ghenniwa and J. Samarabandu. Risk-based modelling for managing privacy protection. Presented at Electrical & Computer Engineering (CCECE), 2012 25th IEEE Canadian Conference On. 2012 .

[5]. A.Datta, J. Blocki, N. Christin, H. DeYoung, D. Garg, L. Jia, D. Kaynar and A. Sinha. Understanding and protecting privacy: Formal semantics and principled audit mechanisms. Presented at Proceedings of the 7th International Conference on Information Systems Security. 2011, Available: http://dx.doi.org/10.1007/978-3-642-25560-1_1. DOI: 10.1007/978-3-642-25560-1_1.

[6]. A.Huertas Celdran, F. J. Garcia Clemente, M. Gil Perez and G. Martinez Perez. SeCoMan: A semantic-aware policy framework for developing privacy-preserving and context-aware smart applications. *Systems Journal, IEEE PP(99)*, pp. 1-14. 2014. . DOI: 10.1109/JSYST.2013.2297707.

[7]. A.Krause and E. Horvitz. A utility-theoretic approach to privacy and personalization. Presented at Proceedings of the 23rd National Conference on Artificial Intelligence - Volume 2. 2008, Available: http://dl.acm.org/citation.cfm?id=1620163.1620256.

[8]. A.Machanavajjhala, D. Kifer, J. Gehrke and M. Venkitasubramaniam. L-diversity: Privacy beyond k-anonymity. *ACM Trans.Knowl.Discov.Data 1(1),* 2007. Available: http://doi.acm.org/10.1145/1217299.1217302. DOI: 10.1145/1217299.1217302.

[9]. A.Singla, E. Horvitz, E. Kamar and R. W. White. Stochastic privacy. Presented at Proc. Conference on Artificial Intelligence (AAAI). 2014,

[10]. A.Ukil, S. Bandyopadhyay, J. Joseph, V. Banahatti and S. Lodha. Negotiation-based privacy preservation scheme in internet of things platform. Presented at Proceedings of the First International Conference on Security of Internet of Things. 2012, Available: http://doi.acm.org/10.1145/2490428.2490439. DOI: 10.1145/2490428.2490439.

[11]. A.Westin, *Privacy and Freedom.* 1967.

[12]. Acquisti, A., C. R. Taylor, and L. Wagman (2016). The economics of privacy. Forthcoming, Journal of Economic Literature.

[13]. Aleisa, N. and Renaud, K. (2017). Privacy of the Internet of Things: A Systematic Literature Review (Extended Discussion).

[14]. Anonymous *Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence* 1999.

[15]. B.Faltings, T. Leaute and A. Petcu. Privacy guarantees through distributed constraint satisfaction. Presented at Web Intelligence and Intelligent Agent Technology, 2008. WI-IAT '08. IEEE/WIC/ACM International Conference On. 2008, . DOI: 10.1109/WIIAT.2008.177.

[16]. B.K. Sy, A. Ramirez and A. P. K. Krishnan. Secure information processing with privacy assurance - standard based design and development for biometric

applications. Presented at Privacy Security and Trust (PST), 2010 Eighth Annual International Conference. 2010, . DOI: 10.1109/PST.2010.5593255.

[17]. B.Kepes, "Understanding-the-Cloud-Computing-Stack," *Rackspace White Paper*, 2011.

[18]. Bo Lang , Ian Foster , Frank Siebenlist , Rachana Ananthakrishnan , Tim Freeman, "A Multipolicy Authorization Framework for Grid Security," *Proceedings of the Fifth IEEE Symposium on Network Computing and Application,* 2006.

[19]. C.Clifton and T. Tassa. On syntactic anonymity and differential privacy. *2013 IEEE 29th International Conference on Data Engineering Workshops (ICDEW) 0*pp. 88-93. 2013. . DOI: http://doi.ieeecomputersociety.org/10.1109/ICDEW.2013.6547433.

[20]. C.Dwork. Differential privacy: A survey of results. Presented at Proceedings of the 5th International Conference on Theory and Applications of Models of Computation. 2008, Available: http://dl.acm.org/citation.cfm?id=1791834.1791836.

[21]. C.N. and S. J.M. Implicit contextual integrity in online social networks. *ArXiv E-Prints* 2015. Available: http://adsabs.harvard.edu/abs/2015arXiv150202493C.

[22]. D.J. Solove, M. Rotenberg and P. M. Schwartz. *Privacy, Information and Technology* 2006Available: http://books.google.ca/books?id=Ze3_NDCHK2IC.

[23]. D.J. Solove. *Nothing to Hide: The False Tradeoff between Privacy and Security* 2011Available: http://books.google.ca/books?id=UUdQi4FxRxAC.

[24]. D.J. Solove. *Understanding Privacy* 2008*(v. 10).* Available: http://books.google.ca/books?id=XU5-AAAAMAAJ.

[25]. D.Lake, R. Milito, M. Morrow and R. Vargheese, "Internet of Things: Architectural Framework for eHealth Security," 2013.

[26]. Digital Engagement Experience https://www.dexit.co/

[27]. Dwork, C. and Roth, A. (2013). The Algorithmic Foundations of Differential Privacy. *Foundations and Trends® in Theoretical Computer Science,* 9(3-4), pp.211-407.

[28]. E.L. Godkin, "Libel and its Legal Remedy."  pp. 80, 1880.

[29]. F.P. Calmon, “Information-theoretic metrics for security and privacy,” Ph.D. dissertation, MIT, Sep. 2015.

[30]. Farrell, J. (2012). Can privacy be just another good. J. on Telecomm. & High Tech. L. 10, 251.Privacy, Algorithms and Artificial Intelligence.

[31]. Gupta, P., Tyagi, V. and Kumar Singh, S. (2017). *Cloud-Based Information Security*.

[32]. H.H. Ghenniwa, "Coordination in Cooperative Distributed Systems,"  1996.

[33]. H.Lee and M. Stamp. An agent-based privacy-enhancing model. 2008, .

[34]. H.Tian and W. Zhang. Privacy-preserving data publishing based on utility specification. Presented at Social Computing (SocialCom), 2013 International Conference On. 2013, DOI: 10.1109/SocialCom.2013.24.

[35]. H.Vanchinathan, G. Bart\'ok and A. Krause. Efficient partial monitoring with prior information. Presented at Neural Information Processing Systems (NIPS). 2014.

[36]. *HOW MUCH DATA IS CREATED EVERY MINUTE?*. Available: http://www.visualnews.com/2012/06/19/how-much-data-created-every-minute/ (June 2012).

[37]. I.Kayes and A. Iamnitchi. Aegis: A semantic implementation of privacy as contextual integrity in social ecosystems. Presented at Privacy, Security and Trust (PST), 2013

Eleventh Annual International Conference On. 2013, . DOI: 10.1109/PST.2013.6596041.

[38]. J.Byun, T. Li, E. Bertino, N. Li and Y. Sohn. Privacy-preserving incremental data dissemination. *J.Comput.Secur. 17(1),* pp. 43-68. 2009. Available: http://dl.acm.org/citation.cfm?id=1517343.1517345.

[39]. J.M. Such, A. Espinosa and A. García-Fornes. A survey of privacy in multi-agent systems. *Knowl. Eng. Rev.* 2012.

[40]. J.Niu and S. Parsons. An investigation report on auction mechanism design. *CoRR abs/0904.1258* 2009.

[41]. JIAC Development Team, "Manual JIAC : Java Intelligent Agent Componentware ," 2014.

[42]. K.Nissim, R. Smorodinsky and M. Tennenholtz. Approximately optimal mechanism design via differential privacy. Presented at Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. 2012, Available: http://doi.acm.org/10.1145/2090236.2090254. DOI: 10.1145/2090236.2090254.

[43]. K.Suzuki and M. Yokoo. Secure combinatorial auctions by dynamic programming with polynomial secret sharing. Presented at In Proceedings of the Sixth International Financial Cryptography Conference. 2002.

[44]. Kate Crawford & Jason Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, 55 B.C. L. REV. 93, 101 (2014)

[45]. L.Crepin, Y. Demazeau, O. Boissier and F. Jacquenet. Sensitive data transaction in hippocratic multi-agent systems. *5485*pp. 85-101. 2009. Available: http://dx.doi.org/10.1007/978-3-642-02562-4_5. DOI: 10.1007/978-3-642-02562-4_5.

[46]. L.Cranor, M. Langheinrich, M. Marchiori, M. Presler-Marshall and J. Reagle, "The Platform for Privacy Preferences 1.0 (P3P1.0) Specification," 2002.

[47]. L.Sweeney. K-anonymity: A model for protecting privacy. *Int.J.Uncertain.Fuzziness Knowl.-Based Syst. 10(5),* pp. 557-570. 2002. Available: http://dx.doi.org/10.1142/S0218488502001648. DOI: 10.1142/S0218488502001648.

[48]. Lambrecht, A. and C. E. Tucker (2015). Can big data protect a firm from competition?. SSRN Electronic Journal.

[49]. M.Bezzi. An information theoretic approach for privacy metrics. *Trans.Data Privacy 3(3),* pp.199-215.2010. Available: http://dl.acm.org/citation.cfm?id=2019307.2019309.

[50]. M.Bezzi. An information theoretic approach for privacy metrics. *Trans. Data Privacy 3(3),* pp. 199-215. 2010. Available:http://dl.acm.org/citation.cfm?id=2019307.2019309.

[51]. M.Gruteser, J. Bredin and D. Grunwald. Path privacy in location-aware computing. 2004.

[52]. M.Naor, B. Pinkas and R. Sumner. Privacy preserving auctions and mechanism design. Presented at Proceedings of the 1st ACM Conference on Electronic Commerce. 1999, Available: http://doi.acm.org/10.1145/336992.337028. DOI: 10.1145/336992.337028.

[53]. M.Tentori, J. Favela and M. D. Rodriguez. Privacy-aware autonomous agents for pervasive healthcare. *IEEE Intelligent Systems 21(6),* pp. 55-62. 2006. Available: http://dx.doi.org/10.1109/MIS.2006.118. DOI: 10.1109/MIS.2006.118.

[54]. M.Tierney and L. Subramanian. Realizing privacy by definition in social networks. Presented at Proceedings of 5th Asia-Pacific Workshop on Systems. 2014, Available: http://doi.acm.org/10.1145/2637166.2637232. DOI: 10.1145/2637166.2637232.

[55]. M.Yokoo, E. H. Durfee, T. Ishida and K. Kuwabara. The distributed constraint satisfaction problem: Formalization and algorithms. *Knowledge and Data Engineering, IEEE Transactions On 10(5),* pp. 673-685. 1998. . DOI: 10.1109/69.729707.

[56]. Masaud-Wahaishi, A. and Ghenniwa, H. (2009). Privacy Based Information Brokering for Cooperative Distributed e-Health Systems. *Journal of Emerging Technologies in Web Intelligence*, 1(2).

[57]. Ninghui Li, Tiancheng Li and S. Venkatasubramanian. T-closeness: Privacy beyond k-anonymity and l-diversity. Presented at Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference. 2007, . DOI: 10.1109/ICDE.2007.367856.

[58]. P.M. Schwartz and D. J. Solove, "*The PII Problem: Privacy and a New Concept of Personally Identifiable Information*," 2011.

[59]. Paul M. Schwartz, Daniel J. Solove. The PII problem: Privacy and a new concept of personally identifiable information. 2011.

[60]. Perera, Charith, et al. "Sensing as a service model for smart cities supported by internet of things." Transactions on Emerging Telecommunications Technologies 25.1 (2014): 81-93.

[61]. R.A. Posner, *The Economics of Justice.* 1981.

[62]. R.Dong, A. A. C\'ardenas, L. J. Ratliff, H. Ohlsson and S. S. Sastry. Quantifying the utility-privacy tradeoff in the smart grid. *CoRR abs/1406.2568*2014. Available: http://arxiv.org/abs/1406.2568.

[63]. R.Greenstadt, J. P. Pearce and M. Tambe. Analysis of privacy loss in distributed constraint optimization. Presented at Proceedings of the 21st National Conference on Artificial Intelligence - Volume 1. 2006, Available: http://dl.acm.org/citation.cfm?id=1597538.1597642.

[64]. R.Greenstadt. An analysis of privacy loss in k-optimal algorithms. Presented at In DCR. 2008,

[65]. S.Bok, *Secrets: On the Ethics of Concealment and Revelation.* 1983.

[66]. S.D. Warren and L. D. Brandies, *The Right to Privacy.* 1890.

[67]. S.Lederer, A. K. Dey and J. Mankoff. A conceptual model and a metaphor of everyday privacy in ubiquitous. University of California at Berkeley. Berkeley, CA, USA. 2002.

[68]. S.Poslad, M. Hamdi and H. Abie. Adaptive security and privacy management for the internet of things (ASPI 2013). Presented at Proceedings of the 2013 ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication. 2013, Available: http://doi.acm.org/10.1145/2494091.2499770. DOI: 10.1145/2494091.2499770.

[69]. S.Singh and S. Bawa. A privacy, trust and policy based authorization framework for services in distributed environments, 2007.

[70]. S.Spiekermann and L. F. Cranor. Engineering privacy. *IEEE Trans. Software Eng. 35(1),* pp. 67-82. 2009. . DOI: http://doi.ieeecomputersociety.org/10.1109/TSE.2008.88.

[71]. Samani, A. (2015). Privacy in Cooperative Distributed Systems: Modeling and Protection Framework.

[72]. Such, J., Espinosa, A. and García-Fornes, A. (2013). A survey of privacy in multi-agent systems. *The Knowledge Engineering Review*, 29(03), pp.314-344.

[73]. Sun, Y., Huang, H., Li, X., Du, Y., Tian, M., Xu, H. and Xiao, M. (2017). Privacy-preserving strategyproof auction mechanisms for resource allocation. *Tsinghua Science and Technology*, 22(2), pp.119-134.

[74]. T.Li and N. Li. On the tradeoff between privacy and utility in data publishing. Presented at KDD} '09: Proceedings of the 15th {ACM} {SIGKDD} International Conference on Knowledge Discovery and Data Mining. 2009, . DOI: http://doi.acm.org.library.capella.edu/10.1145/1557019.1557079.

[75]. Tucker, C. (2017). Privacy, Algorithms and Artificial Intelligence.

[76]. V. Toubiana, H. Nissenbaum, A. Narayanan, S. Barocas and D. Boneh. Adnostic: Privacy preserving targeted advertising ∗. 2010.

[77]. Y.D. Wang. Ontology-driven semantic transformation for cooperative information systems. 2009.

[78]. Zagaratnam , J. Dayka , A. Nadalin , F. Siebenlist , V. Welch , I. Foster , S. Tuecke, "The Security Architecture for Open Grid Services," 2002.

[79]. Ziegeldorf, J., Morchon, O. and Wehrle, K. (2013). Privacy in the Internet of Things: threats and challenges. Security and Communication Networks, 7(12), pp.2728-2742.

# Curriculum Vitae

| | |
|---|---|
| **Name:** | Ali Fouad Saleh |
| **Post-secondary M.E.Sc.** | (2015-2018) |
| **Education and Degrees:** | Electrical and Computer Engineering<br>Western University<br>London, Canada |

**Advanced Diploma. (2008-2012)**
Information Systems Management
The Higher Institute of Computer Techniques / Benghazi, Libya

**Scholarships:** The Ministry of Higher Education of Libya funding for the Libyan-North American Scholarship Program.

**Related Work**:

- Software Testing and Quality team – Internship
    - Digital Engagement Experience (DEX), London, ON.
      2016 – 2018
- Teaching Assistant
    - Electronic and Computer Engineer
      The University of Western Ontario, London, ON.
      2016
- Teaching Assistant.
    - Information Systems Management Department of the Higher Institute of Computer Techniques / Benghazi, Libya
      2012-2014
- IT Officer
    - International Medical Corps (IMC) – Libya
      IT Department
      2011-2014
- Technical Support Officer
    - Al-Ala Company - Computer Services and Technical Consulting
      2011-2014