EVALUATION OF TRUST IN THE INTERNET OF THINGS: MODELS, MECHANISMS AND APPLICATIONS

NGUYEN BINH TRUONG

A thesis submitted in partial fulfilment of the requirements of Liverpool John Moores University for the degree of Doctor of Philosophy

August 2018

DECLARATION

I, Nguyen Binh Truong, confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm this has been indicated in the thesis.

Nguyen Binh Truong

Word count (Excluding acknowledgement, appendices and references): 44,460 **words**
(excluding the Appendixes and References)

ACKNOWLEDGEMENT

I take this opportunity to express my gratitude to everyone who supported me throughout my PhD study.

Firstly, I would like to express my sincere gratitude to my supervisors Dr. Gyu Myoung Lee, Dr. Bo Zhou and Dr. Bob Askwith for the continuous support during my PhD and related research, for their patience, motivation, and immense knowledge. Their guidance helped me in all the time of doing research and writing of this thesis. I consider myself fortunate to be one of their students and I will forever be indebted to each of them. I could not have imagined having a better supervisors and mentors for my PhD study. I extend my deepest appreciation to Dr. Gyu Myoung Lee for encouraging me to undertake a research degree and for his never-ending advice, expertise and support throughout my PhD study. The support and guidance I received from Dr. Lee has been invaluable and has pushed me to move to the boundaries of the research and to reach my abilities. He has also allowed me to develop as an independent researcher for my future career.

I wish to thank my amazing wife Anh Tran for her support, patience and understanding throughout my PhD. I thank her for giving me the determination to work hard each and every day. Also, I wish to express special thanks to the staff and technicians at the faculty, Ms. Tricia Waterson for her endless advice and support and Ms. Carol Oliver for always getting me to those conferences.

Finally, I would like to thank my colleagues Upul Jayasinghe, Ali Alfoudi and Mohammed Dighriri. It would have been impossible to do my job and my PhD without the support of these colleagues and friends. I thank them for their understanding and willingness to endure more work as a result of my studies.

ABSTRACT

In the blooming era of the Internet of Things (IoT), trust has become a vital factor for provisioning reliable smart services without human intervention by reducing risk in autonomous decision making. However, the merging of physical objects, cyber components and humans in the IoT infrastructure has introduced new concerns for the evaluation of trust. Consequently, a large number of trust-related challenges have been unsolved yet due to the ambiguity of the concept of trust and the variety of divergent trust models and management mechanisms in different IoT scenarios.

In this PhD thesis, my ultimate goal is to propose an efficient and practical trust evaluation mechanisms for any two entities in the IoT. To achieve this goal, the first important objective is to augment the generic trust concept and provide a conceptual model of trust in order to come up with a comprehensive understanding of trust, influencing factors and possible Trust Indicators (TI) in the context of IoT. Following the catalyst, as the second objective, a trust model called REK comprised of the triad Reputation, Experience and Knowledge TIs is proposed which covers multi-dimensional aspects of trust by incorporating heterogeneous information from direct observation, personal experiences to global opinions. The mathematical models and evaluation mechanisms for the three TIs in the REK trust model are proposed. Knowledge TI is as “direct trust” rendering a trustor’s understanding of a trustee in respective scenarios that can be obtained based on limited available information about characteristics of the trustee, environment and the trustor’s perspective using a variety of techniques. Experience and Reputation TIs are originated from social features and extracted based on previous interactions among entities in IoT. The mathematical models and calculation mechanisms for the Experience and Reputation TIs also proposed leveraging sociological behaviours of humans in the real-world; and being inspired by the Google PageRank in the web-ranking area, respectively.

The REK Trust Model is also applied in variety of IoT scenarios such as Mobile Crowd-Sensing (MCS), Car Sharing service, Data Sharing and Exchange platform in Smart Cities and in Vehicular Networks; and for empowering Blockchain-based systems. The feasibility and effectiveness of the REK model and associated evaluation mechanisms are proved not only by the theoretical analysis but also by real-world applications deployed in our ongoing TII and Wise-IoT projects.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

IoT	**Internet of Things**
TI	Trust Indicator
SIoT	Social Internet of Things
REK	Reputation-Experience-Knowledge
WSN	Wireless Sensor Network
GPS	Global Positioning System
NFC	Near-Field Communication
RFID	Radio Frequency Identification tags
MCS	Mobile Crowd-Sensing
CPSS	Cyber-Physical-Social System
TaaS	Trust as a Service
CPSS	Cyber-Physical-Social System
TA	Trust Attributes
ICT	Information and Communication Technology

CHAPTER 1. INTRODUCTION

With recent advanced technologies moving towards a hyper-connected society from the increasing digital interconnection of humans and objects, big data processing and analysing, the Internet of Things (IoT), applications and services play a significant role in the convenience of human daily life. However various problems due to the lack of trust have been anticipated which hinder the development of the IoT. Trust has been extensively explored in the era of the IoT as an extension of the traditional triad of security, privacy and reliability for offering secure, reliable and seamless communications and services. However, despite a large amount of trust-related research in IoT, a prevailing trust concept, models, and evaluation and management mechanisms have still been debatable and under development. This chapter provides an overview on research of trust in the IoT, challenges, motivation as well as the aims and objectives of my research. The chapter also contains the list of my publications during the PhD period and the structure of the thesis.

1.1 Overview

In recent years, we have been witnessing a novel paradigm – the IoT in which billions of electronic objects are connected. These range from small and low computation capability devices such as Radio Frequency Identification tags (RFIDs) to complex ones like smartphones, smart appliances and smart vehicles. Indeed, the idea to connect and share data among physical objects, cyberspace and people using hyperlinks and over a global network was promulgated by Tim Berners Lee three decades ago. A number of efforts have been made to build upon this premise in the last ten years, for example, Semantic Web (Web 3.0) integrates humans and social information to the Web, yielding a composite Cyber-Social system. With the IoT, we are now reaching to a breakthrough of a Cyber-Physical-Social System (CPSS) that connects the Cyber-Social Webs with physical world objects [1].

With billions of sensing and actuating devices deployed, the IoT is expected to observe various aspects of human life anywhere on Earth. Observation data is aggregated, processed, and analysed into valuable knowledge describing occurrences and events regarding different real-world phenomena. With information from the cyber and social domains, it is possible for a variety of applications and services to reveal the untapped operational efficiencies and create an end-to-end feedback loop between individuals' needs and physical object responses. To do so, a unified CPSS framework should be defined that "takes a human centric and holistic view of computing by analysing observations, knowledge, and experiences from physical, cyber, and social worlds" [2].

In the early years, most IoT-related research articles concentrated on RFID and Wireless Sensor Networks (WSNs) that aim at building underlying networking protocols, hardware and software components in order to enable interactions and communications among physical objects and cyber-space. However, a human-centric IoT environment in which humans play an important role in supporting applications and services, are more and more perceptible. This is proven by the high rate of utilization of social phenomena and crowd intelligence when developing real-world IoT services. People are envisaged as an integral part of the IoT ecosystem [3, 4]. However, the merging of physical objects, cyber components and humans in the IoT will introduce new concerns for risks, privacy and security. Consequently, managing risk and securing the IoT are broad in scope and pose greater challenges than the traditional privacy and security triad of integrity, confidentiality, and availability [5]. In this regard, trust has been recognized as an important role in supporting both humans and services to overcome the perception of uncertainty and risk in decision making.

Trust is a multifaceted concept used in many disciplines in human life influenced by both participants and environmental factors. It is an underlying psychological measurement to help a trustor to come up with a decision whether it should put itself into a risky situation in case a trustee turns out to be misplaced. Currently, IoT ecosystems have been built upon a riddle of physical objects and networking devices, wrapped in an enigma of protocols and protected by sets of incoherent security and privacy mechanisms. The merging of physical objects, cyber components and especially humans will introduce new concerns for risks, privacy and security at all infrastructure, services and society levels. Therefore, having evaluation of trust could minimize the unexpected risks and maximize the predictability, which helps both IoT infrastructures and services to operate in a controlled and autonomous manner and to avoid unpredicted conditions and service failures.

1.2 Problem Statement and Research Motivation

Many research groups are working on trust-related areas in various environments varying in many applications from access control [6] to e-commerce [7, 8]. In such research articles, a variety of trust models and evaluation mechanisms have been proposed; however, they have mainly focused on building reputation systems in social networks for e-Commerce services [9, 10]; or focused on developing trust management mechanisms in distributed systems such as wireless sensor networks (WSNs) [11, 12], mobile ad-hoc networks (MANET) [13-15], and peer-to-peer (P2P) networks [6, 16].

- **Problem Statements:**
  Despite the importance of trust, there are limited notable articles that clearly clarify the trust concept, definition, models and evaluation mechanisms, especially in the IoT environment.

The first problem of the state-of-the-art trust-related research is the lack of deep understanding on the concept of trust and the evaluation of trust, particularly in the IoT environment. That is why a large number of articles have confused between reputation and trust; and have unconsciously used reputation as trust. Also, trust is calculated based on some information without any explanation and strong reasons. An evaluation of trust based on insufficient or irrelevant features will lead to biased and incorrect results, and consequently depresses IoT systems' operation and quality of applications and services, even imposing vulnerability and threats to the systems and services.

The second problem is the limitation of a comprehensive and consistent evaluation mechanism for trust. A trust evaluation mechanism needs to deal with three questions: "What kind of information is needed to evaluate trust?", "how is the information obtained or extracted?" and "how is the information aggregated to compute an overall trust value?" The difficulties of trust evaluation are mainly due to three reasons. The first is the lack of a conceptual evaluation model that contains necessary and sufficient Trust Indicators (TIs) and associated attributes to compute an overall trust value. The second is the huge, complex and multi-dimensional data collected from various kinds of resources in a multi-layer network environment resulting in the uncertainty of information and the difficulty in information selection and extraction. The third reason is the difficulty in aggregating trust information; the difficulty in combining information for deriving the TIs and the overall trust value, respecting the personalized and subjective trust.

- **Research Motivation**

The research in this thesis is motivated by the significant challenges on the concept, the model and the evaluation mechanisms of trust in the IoT environment. Given the state-of-the-art, each of the previous related research papers is as a separated piece of a big picture of trust evaluation dealing with a challenge in a specific environment. Due to the diversity of applications and their inherent differences in nature, trust is hard to formalize in a general setting, and up to now no commonly accepted model has appeared. Thus, the ultimate motivation is to generalize a concept of trust in the IoT environment as well as to provide a standard model and efficient mechanisms for evaluating trust in the IoT. This research work is expected as a catalyst for trust-related research as well as real implementation of the evaluation mechanisms.

The motivation is also drawn from the necessity of providing a trusted platform for interactions among both humans and systems in a variety of use-cases and scenarios; consequently, encouraging online transactions while reducing vulnerabilities, threats and risks in IoT systems, applications and services. The final goal is to develop a trust platform operating as a core-service (i.e., Trust as a Service (TaaS)) that cooperates with IoT systems and services to help both service consumers and providers to acquire trust, resulting in more secure activities and providing better quality of services and experiences.

1.3 Research Aims and Objectives

There are two main aims in the thesis. The first aim is to investigate a conceptual evaluation model of trust in the IoT which illustrates the understanding of the trust concept, introducing a novel concept called Trust Indicators (TIs) and the related Trust Attributes (TAs). The second aim is to come up with the algorithms and mechanisms for evaluating trust in the IoT based on the investigation of the model in the first aim.

To fulfil the aims, the objectives of this research are presented as follows:

(1) Investigate State of the art Trust Concepts, Models and Evaluation mechanisms

Review and comprehend different trust concepts, models, and evaluation and management mechanisms in accordance with the latest research work in both computer science and social science, in addition to initialising an overall understanding and among different perspectives of trust.

(2) Investigate Trust Evaluation and Management approaches in various scenarios and environments

Explore trust evaluation and management approaches and mechanisms in different conditions and environments such as P2P, WSNs, E-commerce and Web services, and distributed systems which might be migrated in the IoT environment. Investigate and identify challenges, pros and cons of the approaches in order to comprehend whether the approaches can be utilized and improved.

(3) Propose a trust concept, a generalized conceptual evaluation model for trust, and the REK trust evaluation mechanisms in the IoT

A novel concept of trust in the IoT is considered, regarding a variety of features and influenced factors of trust in the IoT environment based on the literature review. A conceptual evaluation model for trust is also provided that is generalized and can be used in various scenarios in the IoT. The conceptual evaluation model takes into account and lists up potential TIs and associated attributes as references that could be used in different scenarios. As an important objective, a standard evaluation model called REK is proposed leveraging the conceptual model that specifies necessary and sufficient TIs along with related attributes in detail.

(4) Design and Develop Mechanisms for the REK Evaluation Model

The REK trust evaluation model comprises of a triad of Reputation, Experience and Knowledge TIs. In order to evaluate these TIs, mathematical models and evaluation mechanisms are designed and developed, respecting the imitation of the social cognition of trust in humans, which is based on (i) public opinion as Reputation; (ii) previous interactions (as Experience); and (iii) understandings (as Knowledge).

(5) Use-Cases Demonstration and Deployment

Finally, one of the important objectives is the utilization of the trust evaluation mechanisms in a variety of scenarios considering the IoT environment. The REK model is implemented and demonstrated in Smart City scenarios, MCS systems, and a Blockchain-based platform, showing efficiency to be deployed in reality. The REK evaluation model is also integrated in a real-world IoT service called Smart Parking as a proof of the feasibility of the proposed mechanisms.

Objective	**Methodology**
(1) Investigate State of the art Trust Concepts, Model and Mechanisms	Conducting literature review of trust concepts, model, related properties and attributes, and mechanisms in both Social Science and Computer Science
(2) Investigate Trust Evaluation and Management approaches in various scenarios and environments	Conducting literature review of evaluation and management algorithms and mechanisms on both trust, reputation, and ranking fields.
(3) Design a trust concept, a generalized conceptual evaluation model for trust, and the REK trust evaluation mechanisms in the IoT	Theoretical conceptual evaluation model in accordance with the IoT system model considering Weighted Sum, Fuzzy Logic, and Reasoning techniques
(4) Design and Develop Algorithms and Mechanisms for the REK Evaluation Model	Aggregation techniques for Knowledge TI Mathematical Models for Experience TI PageRank-based Graph-theory techniques for Reputation TI
(5) Use-Cases Demonstration and Deployment	Both Simulation (Matlab) and Implementation (Web Service platform) for the proposed mechanisms

1.4 Research Contributions

This research provides three major contributions. The first contribution is the augmentation of the trust concept, definition and conceptual evaluation model that consolidates understanding on trust in the IoT environment. The second contribution is the introduction of a conceptual trust evaluation mechanism in the IoT environment called REK which comprises the three components Reputation, Experience and Knowledge. Mathematical models and evaluation mechanisms for the three components are proposed and described along with an aggregation mechanism for integrating the three components to finalize a trust value. The third contribution is the utilisation of the proposed REK model in some use-cases in the IoT environment such as Smart Cities, Mobile Crowd-Sensing (MCS) [17] and Blockchain-based systems.

(1) A Novel Trust Concept, Trust Definition and Conceptual Evaluation Model in the IoT:

This is novel since it reflects the IoT characteristics in trust and helps to remove the confusion among trust, reputation, dependability, security and privacy.

- A novel trust concept and definition in the IoT environment considering the trilogy Trustor's propensity, Trustee's trustworthiness and Environment's characteristics.
- A trust evaluation conceptual model specifying the concept of TIs, respecting the trilogy Trustor's propensity, trustee's trustworthiness and environment's characteristics.

(2) REK Evaluation Model and Mechanisms:

This evaluation model is novel due to the integration of Knowledge, Experience and Reputation in a reasonable manner imitating the behaviours of human in social science. The Experience mathematical model and the PageRank-based reputation calculation successfully illustrate the Trust concept in the IoT.

- The REK Trust Evaluation model specifies the triad of TIs namely Reputation, Experience and Knowledge.
- Fuzzy Logic and Reasoning Mechanism for the Knowledge TI
- Mathematical Model and calculation algorithm for the Experience TI
- Mathematical Model and calculation algorithm for the Reputation TI

(3) Utilisation of the REK Evaluation Model in various Use-cases

With the novelty from the REK trust model, the utilisation of the associated evaluation mechanisms reflects emerging contributions to different scenarios in IoT environment

- Analysis of the Knowledge-based Trust Evaluation in Car Sharing use-case using Fuzzy Logic

- Analysis and Prototype of the Knowledge-based Trust Evaluation in Data Sharing in Smart Cities using Reasoning mechanism and Inference Engine
- Employment and Implementation of the REK Trust Evaluation mechanisms in Mobile Crowd-Sensing systems in the IoT
- Employment of the REK Trust Evaluation in Blockchain-based Systems
- Real-world Implementation and Deployment of the proposed REK Trust Evaluation mechanisms in the Smart Parking service in Smart Cities

(4) Standardization:

We aim at supporting the ITU-T standardization body our research work on trust, which is important contributions for industry. Based on the technical reports related to Trust, algorithms and mechanisms, industrial partners could have insight on how to provide trusted devices, platforms, systems and services.

After developing the technical report on trust in the Correspondence Group on Trust (CG-Trust), ITU-T SG13 has started to develop related recommendations. As the initial stage, Q16/13 agreed to develop a new draft Recommendation on "Overview of trust provisioning in ICT infrastructures and services". We has lead the standardization on trust definition, features and social-cyber-physical trust in this Recommendation. Detailed of the Standardization contributions can be found in Appendix C.

1.5 List of Publications

During the PhD period, I have published and submitted some papers to top conferences such as IEEE Global Communications (GLOBECOM), IEEE International Conference on Communication (ICC), IEEE TRUSTCOM, IFPF/IEEE Innovations in Clouds, Internet and Networks (ICIM), and IFPF/IEEE Integrated Network and Service Management (IM), and high-ranked journals such as SENSORS journal, IEEE Transaction on Information Forensics Security, and IEEE Internet Computing Magazine. I have also intensively contributed to the ITU-T standardisation body from the beginning of the PhD period until now. I have had some opportunities to give presentations and talks at some of these conferences (IEEE GLOBECOM, IFPF/IEEE ICIN, IEEE Smart World Congress) and workshops in University of Oxford and in Liverpool John Moores University.

Details of my publications can be found in Google Scholar[1]. During the PhD period, I have gained more than 150 citations for the published papers, which indicates the quality and the influence of the research work, novelty and the contributions presented in this PhD thesis.

[1] https://scholar.google.com/citations?user=mj4CTOgAAAAJ&hl=en

❖ Conferences

2018 [C8] Hamza Baqa, **Nguyen B. Truong**, Noel Crespi, Gyu Myoung Lee, Franck Le Gall, "*Quality of Information as an indicator of Trust in the Internet of Things*", IEEE International Conference on Trust, Security And Privacy In Computing And Communications (IEEE TrustCom), New York, U.S.A, July 2018.

[C7] **Nguyen B. Truong**, Tai-Won Um, Bo Zhou, and G. M. Lee, "*Strengthening the Blockchain-based Internet of Value with Trust*", IEEE International Conference on Communications (ICC), Kansas, U.S.A, May 2018.

2017 [C6] **Nguyen B. Truong**, Tai-Won Um, Bo Zhou, and G. M. Lee, "*From Personal Experience to Global Reputation for Trust Evaluation in the Social Internet of Things*", IEEE Global Communications Conference (GLOBECOM), Singapore, December 2017.

[C5]. **Nguyen B. Truong**, Gyu Myoung Lee, *"Trust Evaluation for Data Exchange in Vehicular Networks",* IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), Pittsburgh, PA, USA, April 2017

2016 [C4]. **Nguyen B. Truong**, Quyet H. Cao, Tai-Won Um, Gyu Myoung Lee, *"Leverage a Trust Service Platform for Data Usage Control in Smart City",* IEEE Global Communications Conference (GLOBECOM), Washington DC, USA, December 2016.

[C3]. Upul Jayasinghe, **Nguyen B. Truong**, Tai-Won Um, Gyu Myoung Lee, *"RpR: A Trust Computation Model for Social Internet of Things"*, IEEE Smart World Congress, Toulouse, France, July 2016.

[C2]. **Nguyen B. Truong,** Tai-Won Um, Gyu Myoung Lee, *"A Reputation and Knowledge Based Trust Service Platform For Trustworthy Social Internet of Things*", IFIP/IEEE Innovations in Clouds, Internet and Networks (ICIN), Paris, France, March 2016.

2015 [C1]. **Nguyen B. Truong**, Gyu Myoung Lee, Y. Ghamri-Doudane, *"Software Defined Network-based Vehicular Adhoc Network with Fog Computing"*, IFIP/IEEE Symposium on Integrated Network and Service Management 2015 (IM 2015), Ottawa, Canada, May 2015.

❖ Journals

2018 [J4]. **Nguyen B. Truong**, A. Jara and G. M. Lee, *“Strengthening Data Accountability in Smart Cities with Blockchain and Smart Contracts”,* IEEE Internet Computing Magazine, Submitted, June 2018.

[J3]. **Nguyen B. Truong**, Tai-Won Um and G. M. Lee, “*Trust Evaluation Mechanism for User Recruitment in Mobile Crowd-Sensing in the Internet of Things*”, IEEE Internet of Things Journal, Submitted, May 2018.

2017 [J2]. **Nguyen B. Truong**, H. Lee, B. Askwith, and G. M. Lee, “Toward a trust evaluation mechanism in the social internet of things”, SENSORS, vol. 17, no. 6, p. 1346, 2017

2016 [J1]. **Nguyen B. Truong**, Upul Jayasinghe, Tai-Won Um, Gyu Myoung Lee, *“A survey on trust computation in the Internet of Things*”, The Korean Institute of Communications and Information Sciences, Information and Communications Magazine, ISSN 1226-4275, vol.32, no. 2, pp.10-27, February 2016.

❖ Talks and Presentations

12/2017 **IEEE Global Communication Conference (GLOBECOM)**, Singapore: *“From Personal Experience to Global Reputation for Trust Evaluation in the Internet of Things”.*

09/2017 **Symposium on Spatial Networks, Engineering and Physical Sciences Research Council, University of Oxford***,* Oxford, U.K: *Experience and Reputation in the Evaluation of Trust in Social Networks”.*

12/2016 **IEEE Global Communication Conference (GLOBECOM)**, Washington DC, USA: *“Leverage a Trust Service Platform for Data Usage Control in Smart City”.*

07/2016 **IEEE Smart World Congress**, Toulouse, France: *“RpR: A Trust Computation Model for Social Internet of Things”.*

04/2016 **Faculty Research Week, Faculty of Engineering and Technology, Liverpool John Moores University**, Liverpool, U.K: *“Trust in Data Sharing for the future Internet of Things”.*

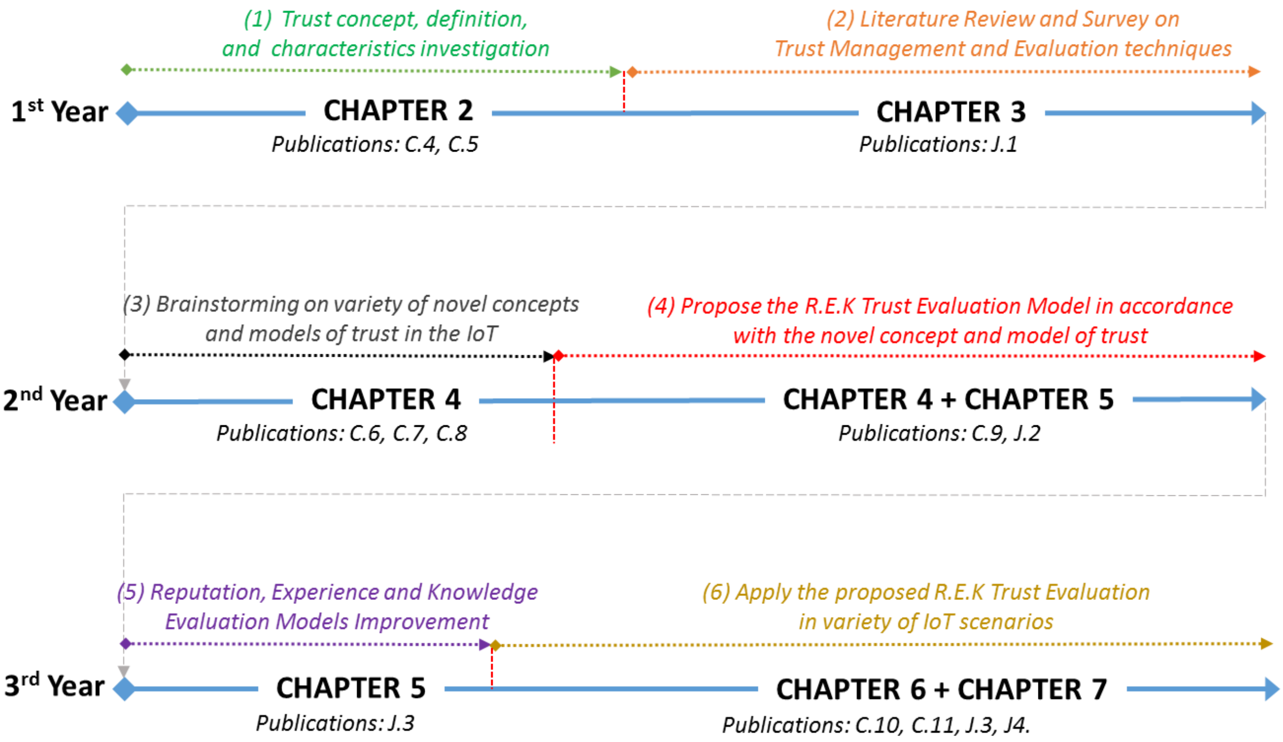
03/2016 **IFIP/IEEE Innovations in Clouds, Internet and Networks (ICIN) Conference**, Paris, France: *“A Reputation and Knowledge Based Trust Service Platform for Trustworthy Social Internet of Things*”.

11/2013 **IEEE Military Communications Conference (MILCOM),** California, USA: *"Latency Analysis in GNU Radio/USRP-based Software Defined Radio Platform"*.

10/2008 **Pacific Rim International Conferences on Artificial Intelligence (PRICAI)**, Hanoi, Vietnam: *"New Particle Swarm Optimization Algorithm for Solving Bounded Degree Minimum Spanning Tree Problem"*.

1.6 Structure of the Thesis

This organization of the thesis is generally following the research track that we have decided from the beginning of my PhD study. Figure 1-1 illustrates the thesis organization with related information including research topics for each PhD milestones and publications. In this figure, in the Publications information under each topic, the notation *C.x* stands for conference paper number *x*; the notation *J.y* stands for the journal paper number *y* in the List of Publication.



(1) Trust concept, definition, and characteristics investigation
(2) Literature Review and Survey on Trust Management and Evaluation techniques
1st Year
CHAPTER 2
Publications: C.4, C.5
CHAPTER 3
Publications: J.1
(3) Brainstorming on variety of novel concepts and models of trust in the IoT
(4) Propose the R.E.K Trust Evaluation Model in accordance with the novel concept and model of trust
2nd Year
CHAPTER 4
Publications: C.6, C.7, C.8
CHAPTER 4 + CHAPTER 5
Publications: C.9, J.2
(5) Reputation, Experience and Knowledge Evaluation Models Improvement
(6) Apply the proposed R.E.K Trust Evaluation in variety of IoT scenarios
3rd Year
CHAPTER 5
Publications: J.3
CHAPTER 6 + CHAPTER 7
Publications: C.10, C.11, J.3, J4.

Figure 1-1. Thesis organization in accordance with the research tracks, topics and publications

In detail, this thesis is organised in eight chapters as follows:

- Chapter 1 introduces the research problem along with the aims and objectives of this study. It also describes the contributions and list of publication; and outlines the structure of the PhD thesis.

- Chapter 2 introduces background and necessary knowledge on trust in Computer Science in general including concept, model, characteristics, and provisioning of trust in the IoT.
- Chapter 3 reviews the trust-related literature to investigate recent studies that target different concepts and models along with evaluation and management mechanisms of trust in a variety of scenarios. This chapter contrasts and compares these studies to explore their advantages and drawbacks; as well as to determine the research gaps and potential research directions.
- Chapter 4 presents a novel trust concept in the IoT and clarifies related aspects of trust in the IoT. In this chapter, a conceptual model for trust evaluation is also proposed along with a brief introduction of the proposed REK trust evaluation model.
- Chapter 5 describes all proposed mathematical models, mechanisms and analysis of the three TIs, namely Knowledge, Experience and Reputation, in the proposed REK trust evaluation models. The chapter ends with the description of several methodologies for aggregating the three TIs to obtain overall trust values as the final goal of the REK model.
- Chapter 6 and Chapter 7 are dedicated to the utilisation of the proposed REK Trust Evaluation model in a variety of scenarios and use-cases. Chapter 6 focuses on the employment of the REK model and implements a trust evaluation mechanism to MCS systems. The trust evaluation mechanism is leveraged for a proposed trust-based User Recruitment scheme in an MCS platform for recruiting trustworthy users in MCS systems. Details of the trust mechanism, the trust-based User Recruitment scheme, analysis and results are also presented.
- Chapter 7 introduces utilisations of the proposed REK model in other scenarios and use-cases such as Car Sharing service, Data Sharing in Smart Cities, and in Blockchain-based systems. Especially, the REK evaluation model is employed and practically deployed in the Smart Parking use-case in Smart Cities, which is a real-world service deployed in the City of Santander, Spain.
- Chapter 8 concludes this study with recommendations for potential future work.

CHAPTER 2. BACKGROUND ON TRUST

2.1 Introduction

Trust is a complex notion and a multi-level analysis is important in order to understand it. This chapter aims to introduce some fundamental knowledge on trust, including concept, definition, characteristics and attributes of trust, particularly in IoT environment. Trust in the digital world interplays between social science and computer science, affected by both objective and subjective factors such as system attributes and social relations [18]. At the deeper level, trust is regarded as a consequence of progress towards security or privacy objectives. Trust is not a new research topic in computer science, spanning areas as diverse as security and access control in computer networks, reliability in distributed systems, game theory and agent systems, and policies for decision making under uncertainty. The concept of trust in these different communities varies in how it is represented, evaluated, and used.

2.2 Trust Concept and Trust Model in Computer Science

As trust can be interpreted in different ways, here we present various meanings from literature for more clear views on trust in terms of telecommunication systems and show relationships between knowledge and trust. Generally speaking, trust means reliance on the integrity, strength, ability, surety, etc., of a person or object. Generally, trust is used as a measure of confidence that an entity will behave in an expected manner, despite the lack of ability to monitor or control the environment in which it operates. Trust in computer science in general can be classified into two broad categories: “user” and “system”. The notion of “user” trust is derived from psychology and sociology, with a standard definition as “a subjective expectation an entity has about another’s future behaviour”. “System” trust is “the expectation that a device or system will faithfully behave in a particular manner to fulfil its intended purpose”.

Trust concept is an abstract notion with different meanings depending on both participants and scenarios; and influenced by both measurable and non-measurable factors. There are various kinds of trust definitions leading to difficulties in establishing a common, general notation that holds, regardless of personal dispositions or differing situations. Generally, trust is considered as a computational value depicted by a relationship between trustor and trustee, described in a specific context and measured by trust metrics and evaluated by a mechanism. Previous research has shown that trust is the interplay among human, social sciences and computer science, affected by several subjective factors such as social status and physical properties; and objective factors such as competence and reputation [18]. The competence is a measurement of abilities of the trustee to perform a given task which is derived from trustee’s diplomas, certifications and experience. Reputation is formed by the opinion of other entities, deriving from third parties' opinions of previous interactions with the trustee. Trust revolves around ‘assurance’ and confidence that people, data, entities, information or processes will function or behave in expected ways. At the deeper level, trust is regarded as a consequence of progress towards security or privacy objectives.

In most of scenarios including the IoT environment, trust is reliance on the integrity, ability or character of an entity. Trust can be further explained in terms of confidence in the truth or worth of an entity. For example, the EU uTRUSTit[2] project defined that trust is the user’s confidence in an entity’s reliability, including user's acceptance of vulnerability in a potentially risky situation [19]. To understand trust, it is required to analyse the collected data from entities, extract the necessary information for trust; understand the information and then create the trust-related knowledge for the trust computation.

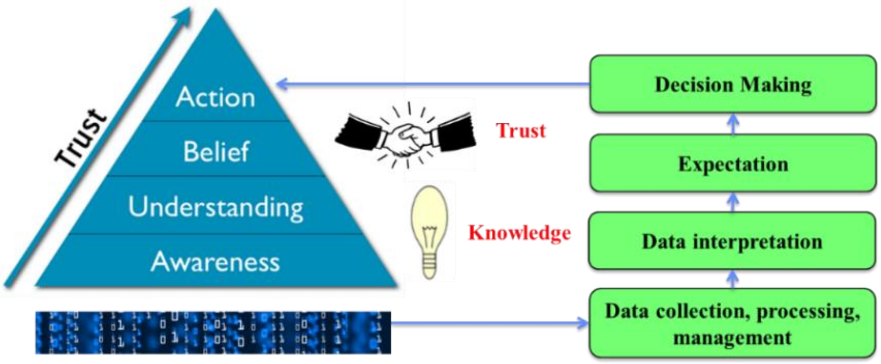


Figure 2-1. Knowledge and Trust

The social and economic value of data is mainly reaped for two moments: first when data is transformed into knowledge (gaining insights) and then when it is used for decision making (taking action). The knowledge is accumulated by individuals or systems through data analytics over time. So far data processing, management and interpretation for awareness and understanding have been considered as fundamental processes for obtaining the knowledge. As shown in Figure 2-1, trust is positioned as belief between knowledge (i.e., awareness and understanding) and action. It means that the expectation process for trust should be additionally considered before decision making.

2.3 Trust in the IoT environment

There are plentiful trust solutions have been proposed for many network systems which are parts of the IoT infrastructure such as P2P, multi-agent systems, and e-commerce. In this section, we consider trust in the IoT: the networks of devices like household appliances, office appliances, sensors and vehicles which are interconnected seamlessly and with self-configuring capability. These electronic devices, which are billions

[2] https://cordis.europa.eu/project/rcn/95532_en.html

in number and varied in size and computing capabilities, are ranging from Radio Frequency Identification tags (RFIDs) to vehicles with On board Units (OBUs). The IoT is expected to enable advanced services and applications like smart home, smart grid or smart city by integrating a variety of technologies in many research areas from embedded systems, wireless sensor networks, service platforms, and automation to privacy, security and trust. With recent advanced technologies moving towards a hyper-connected society from the increasing digital interconnection of humans and objects, big data processing and analysing, the Internet of Things (IoT)-related applications and services are playing a more and more significant role in the convenience of human daily life. However various problems occur due to the lack of trust which will hinder the development of the IoT. To cope with a large number of complex IoT applications and services, it is needed to create a trusted and secured environment in order for sharing information, creating knowledge and conducting transactions.

Therefore, trust in the IoT is a special use-case of trust in Computer Science in which:

- Trustees are normally IoT physical devices, IoT networking systems or IoT services
- Trustors are normally end-users or IoT services that are going to interact with the trustees.
- Variety of properties and characteristics involved such as: the interactions of trustors and trustees in the IoT infrastructure considering three layers of a CPSS: Physical, Cyber and Social layers.
- The trust in IoT involves the human participation as the end-users of IoT applications and services. The human participation plays an important roles in the evaluation of trust by providing feedback, recommendation and reputation.
- The evaluation of trust in the Internet of Things is also different from an evaluation mechanism in Computer Science in general due to the the convergence of two emerging network paradigms, Social Networks and the IoT as Social Internet of Things (SIoT) which has attracted many researchers as a prospective approach for dealing with challenges in the IoT. The benefit of SIoT is the separation in terms of the two levels of humans and devices; allowing devices to have their own social networks; offering humans to impose rules on their devices to protect their privacy and security and maximize trust during the interaction among objects assessing trust is imitated by modulating trust in human society.

Recently, trust in the IoT has been intensively investigated and mostly divided into two types: direct trust and third party trust [20]. The direct trust is a situation where a trusting relationship is nurtured by two entities and formed after these entities have performed transactions with each other. The third-party trust is a trust relationship of an entity that is formed from the third-party recommendations which could mean that no previous transaction had ever occurred between the two interacting entities. For example, entity

A trusts entity B because B is trusted by entity C. In this example, entity A derives trust of B from C, and A also trusts entity C does not lie to him. As with any types of trust relationship, there is a link with the risk which affects the trusting relationship between the entities. The authors in [21] stress that an entity will only proceed with the transaction if the risk is perceived as acceptable.

2.4 Definition of Trust

Trust is a broad concept used in many disciplines and subject areas but until now, there is no commonly agreed definition. It is a critical factor that highly influences the likelihood of entities to interact and transact in both real world and the digital world. Trust is crucial in that it affects the appetite of an entity to use services or products offered by another entity. This example can be seen in our everyday life where trust decisions are made. When purchasing a product, we may favour certain brands or certain models due to our trust that they will provide better quality compare to others. This trust may come from our past experience of using these brands' products (termed "belief") or from their reputations that are perceived from people who bought items and left their opinions about those products (termed "reputation"), or from suggestions of your surrounding such as families and friends (termed "recommendation"). Similarly, trust also affects the decision of an entity to transact with another entity in the same environment. Both consumers and providers should trust each other before decisions to consume or to provide the services are made; otherwise fraudulent transactions may occur.

- **Notion of Trust**

  The trust concept itself is a complicated notion with different meanings depending on both participants and situations and influenced by both measurable and non-measurable factors. There are various kinds of trust definitions leading to difficulties in establishing a common, general notation that holds, regardless of personal dispositions or differing situations. Generally, trust is considered as a computational value depicted by a relationship between trustor and trustee, described in a specific context and measured by trust metrics and evaluated by a mechanism.

  Previous research has shown that trust is the interplay among humans, social sciences and computer science, affected by several subjective factors such as social status and physical properties; and objective factors such as competence and reputation [18]. Competence is the measurement of abilities of the trustee to perform a given task which is derived from the trustee's diplomas, certifications and experience. Reputation is formed by the opinion of other entities, deriving from third parties' opinions of previous interactions with the trustee. Trust may be human to human, machine to machine (e.g. handshake protocols negotiated), human to machine (e.g. when a consumer reviews a digital signature advisory notice) or machine to human (e.g. when a system relies on user input and instructions without extensive verification).

- **Trust Definition**

  It is challenging to concisely define “trust” of an entity due to its uniqueness to each individual entity. Several authors have attempted to define trust from a sociological point of view. They define trust as the trusting behaviour that one person has on another person in a situation where an ambiguous path exists. In such definition, trust is used to mitigate the risks of the dealings with others. Other authors further define trust as the capacity and belief of an entity that the other entity would meet its expectations. However, one of the most prominent works that attempt to derive the notion of trust and was used by many researchers in the online environment is conducted by Gambetta [22]. The authors state that someone is deemed as trustworthy, subject to the probability that he will perform a particular action that is beneficial or non-detrimental for us. This definition is further extended by incorporating the notion of competence along with the predictability. Gambetta *et al.'s* definition on trust is also supported by the author in [23] which further defines trust in an electronic forefront as the competency belief that an agent would act reliably, dependably and securely within a given context. This belief can be quantitatively derived from a subjective probabilistic that an agent has over another in a given period of time. We refer to this definition when discussing about trust throughout this thesis.

2.5 Trust Characteristics and Attributes

Generally, trust presents the confidence and the assurance that entities, users, systems, data and process behave as they are expected to. Therefore, trust can be considered as a way of achieving extra security and privacy objectives. As trust can be interpreted in different ways, here we present various meanings from literature for more clear views on trust in Computer Science [24]. There are several important characteristics of trust that further enhance our understanding about trust in digital environments as following [24]:

- **Trust is dynamic:**

  It applies only in a given time period and may change as time goes by, as it solely depends on the time and changing nature of entities. As an example from the human world, one who was trustworthy some time ago can become changed over time and completely unreliable. For example, for the past one year Alice highly trusts Bob. However, today Alice found that Bob lied to her, consequently, Alice no longer trusts Bob.

- **Trust is context-dependent:**

  Trust applies only in each given context. The degree of trust in different contexts is significantly different. In different contexts trust can be totally unlike and will have different trust measures for each dissimilar scenario. For example, Alice may trust Bob to provide financial advice but not for medical advice.

- **Trust is not transitive in nature but maybe transitive within a given context:**

  That is, if entity A trusts entity B, and entity B trusts entity C, then entity A may not necessarily trust entity C. However, A may trust any entity that entity B trusts in a given context although this derived trust may be explicit and hard to be quantified.

- **Trust is an asymmetric relationship:**

  Thus, trust is non-mutual reciprocal in nature. That means if entity A trusts entity B, then the statement "entity B trusts entity A" is not always true.

The nature of trust is fuzzy, dynamic and complex. Besides asymmetry and transitivity, there are additional key characteristics of trust: implicitness, antonymy, asynchrony, and gravity [25, 26].

- **Implicit:**

  It is hard to explicitly articulate the confidence, belief, capability, context, and time dependency of trust.

- **Antonymy:**

  The articulation of the trust context in two entities may differ based on the opposing perspective. For example, entity A trusts entity B in the context of "buying" a book, however from entity B to entity A the context is "selling" a book.

- **Asynchrony:**

  The period of a trusting relationship may be defined differently between the entities. For example, entity A trusts entity B for 3 years, however, entity B may think that the trust relationship only lasted for the last 1 year.

- **Gravity:**

  The degree of seriousness in trust relationships may differ between the entities. For example, entity A may think that its trust with entity B is important, however, entity B may think differently.

2.6 Trust Provisioning

This section proposes trust taxonomy in different domains in order to identify important issues for trust provisioning in the IoT infrastructure and describes strategies for solving these issues, particularly considering the trust provisioning process. Trust and reputation are the pillars of many social phenomena that shape the Internet socio-economic scene. It is important to have a big picture of Trust in the future IoT in order to successfully develop and deploy trust into applications and services of the IoT infrastructure. Below is the taxonomy providing initial insights into the ways trust benefits can be felt Figure 2-2.

Due to the huge domain of trust usages in the IoT, there are a large number of challenges for designing, developing and deploying a trust platform for systems. We follow the structure of the overall trust taxonomy as illustrated in Figure 2-2 for briefly describing trust provisioning strategies of the IoT infrastructure.

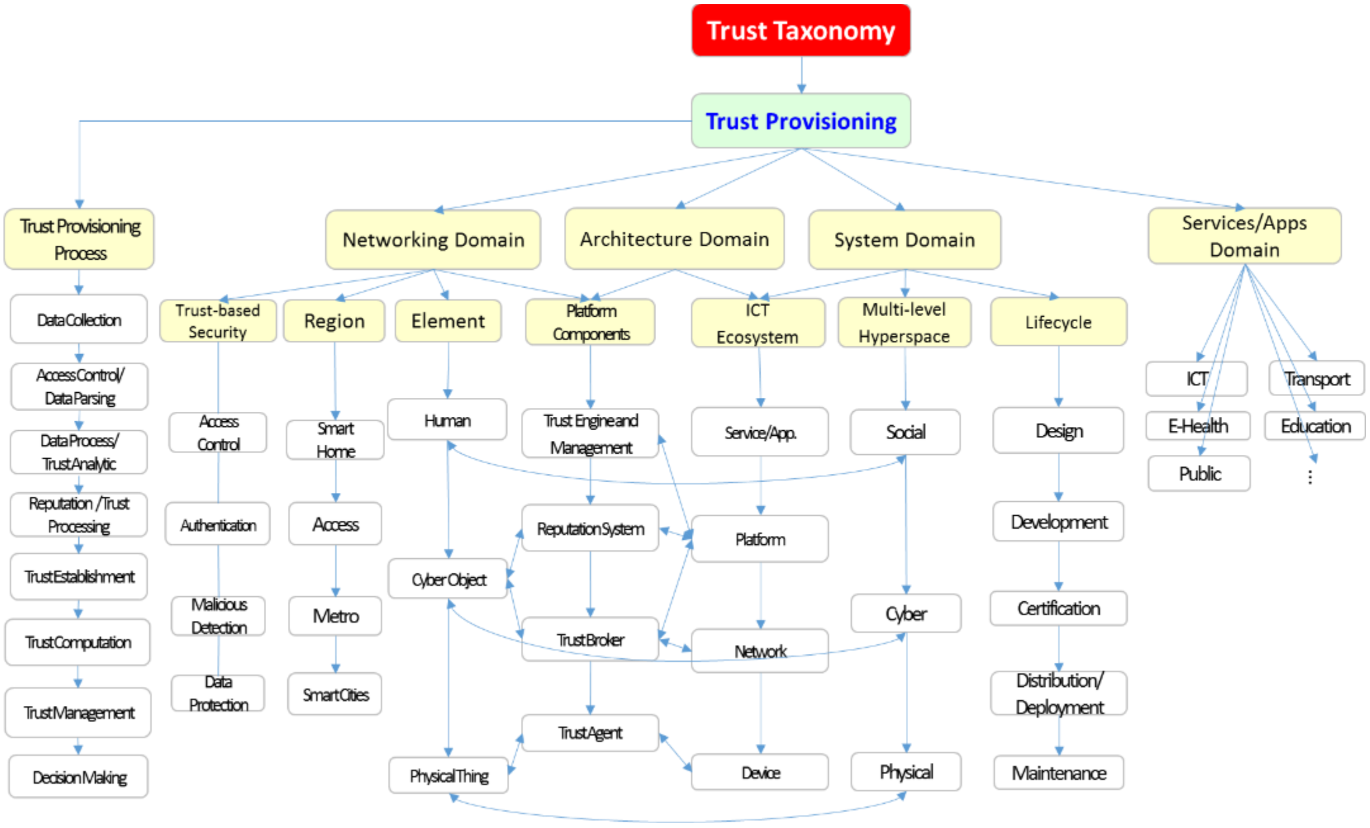


Figure 2-2. Overall Trust Taxonomy in different domains.

Trust is involved in all aspects and in all perspectives of any systems. For example, in the perspective of Networking Domain, trust can be provisioned into Security, Region, and Element aspects as illustrated in the Figure 2-2. We consider four basic domain perspectives, namely Networking Domain, Architecture Domain, System Domain and Services and Applications Domain. In each domain, we consider some aspects in which trust can play a role for better improvements. We also consider trust design, trust development and trust deployment by breaking down to all necessary processes. A trust infrastructure consists of 8 fundamental processes as illustrated in the "Trust Provisioning Process" category in the Trust Taxonomy figure. They are Data Collection, Data Access Control and Data Parsing, Data Process and Trust Analytic, Reputation and Trust Processing, Trust Establishment, Trust Computation, Trust Management and Decision Making.

2.7 Chapter Summary

The term trust in the context of the digital world differs from the concept of trust among people. This notion of trust stands in contrast to some more intuitive notions of trust expressing that someone behaves in a particular well-behaved way. Therefore, this section presents different understandings of trust from various perspectives including concept, definition, characteristics, key features and relationships with knowledge, security and privacy, particularly with respect to both Computer Science and particularly IoT environment.

CHAPTER 3. LITERATURE REVIEW ON TRUST EVALUATION AND MANAGEMENT MECHANISMS

3.1 Introduction

In psychology and sociology, a trust evaluation is a measurement of the degree to which one social actor (an individual or a group) trusts another social actor. Trust evaluation may be abstracted in a manner that can be implemented on computers. Trust escapes a simple measurement because its meaning is too subjective for universally reliable indicators and metrics, and the fact that it is a mental process, unavailable to instruments. There is a strong argument against the use of simplistic methods to measure trust due to the complexity of the process and the 'embeddedness' of trust that makes it impossible to isolate trust from related factors. There is no generally agreed set of properties that make a particular trust indicator better than others, as each method is designed to serve different purposes.

Till now, most research on trust has focused on trust management mechanisms for solving security-related issues such as Access Control in decentralized systems [27, 28], Identity Management [29, 30] and Public Key Certification [31, 32]. In these research works, some network environments are considered such as sensor networks, P2P networks, ad-hoc networks, social networks and the IoT. However, there are limited works on trust evaluation in the IoT environments; and most of them are related to security enhancement for dealing with malicious entities or access control. Nonetheless, the research of trust in the IoT is very necessary due to the need for a trusted environment for the IoT to reach its full potential.

Besides, researchers have also focused on developing trust management mechanisms dealing with trust establishment, dissemination, update and maintenance processes. Some articles have proposed trust evaluation models based on a set of information (so-called direct trust) by extracting a trustee’s characteristics or by observing a trustee’s behaviours. This information is used to describe some trust-related characteristics of an entity that are coined as Trust Attributes (TAs); these TAs are combined into a final value for representing the trustee’s trustworthiness. The trustworthiness is then unconsciously used as trust. Other approaches have measured trust based on third-party information about a trustee that the third-parties have already interacted with, thus, they already gained some clues of trust (so-called indirect trust).

3.2 Overview of Trust Management and Evaluation Mechanisms

A variety of models and mechanisms have been proposed for evaluating trust, however, they have mainly focused on building reputation systems in social networks for e-Commerce services [9],[10] or focused on developing trust management mechanisms in distributed systems such as WSNs [11, 12], mobile ad-hoc networks (MANET) [13-15], and P2P networks [6, 16]. The trust evaluation mechanisms in these articles are mostly based on insufficient information (i.e., only direct observation information or only third-party information). This survey [33] described a detailed discussion about several different trust evaluation methods. Also, the authors in [34] provided certain classification schemes for trust evaluation techniques.

Some trust models attempt to assess trustee's trustworthiness by introducing some TAs and associated evaluation mechanisms for generating a so-called trust. They indeed calculate direct trust that is a portion of the perceived trustworthiness. Researchers have pointed out that in some scenarios such as MANETs, due to high mobility, it is challenging to maintain a centralized system for managing third-party information, resulting in only direct observation information being possibly obtained; and they have to adapt the trust models based on constraints of the environments [13, 14]. In these evaluation models, the direct trust consists of a set of manifold TAs that are necessary and sufficient for a trustor to quantify trust in a particular environment. The perceived trustworthiness is not required to cover all TAs, instead, the set of TAs should be deliberately chosen based on the trustor's propensity and the environmental factors (even though in these articles, the trustor's propensity and the environment characteristics are not mentioned). For example, when evaluating trustworthiness of sensor nodes in WSNs, Bao and Chen have used Cooperativeness, Community-Interest, and Honesty to judge whether a sensor node is malicious or not. These TAs help to evaluate trustworthiness of a sensor node in a WSN that contains some types of vulnerabilities and attacks [11]. The disadvantage of this approach is that the authors do not have a mechanism to combine such information to illustrate the subjectivity of trust. Thus, what they calculate is an instance of an entity's trustworthiness. Y. Yu *et al.* in [12] have analysed various types of threats and attacks and a variety of trust models in the WSN environment for secure routing protocols by characterizing many attributes of a secure system such as security mechanisms and attack preventing mechanisms. Li *et al.* in [15] have used only local information about a node for evaluating trust, giving an incomplete partial trust for trust management called Objective Trust Management Framework (OTMF) in MANETs environment. The novel idea is that they apply a modified Bayesian model using different weights assigned for each piece of information obtained from direct observations. The information is collected using a watchdog mechanism; and in order to calculate weights for each kind of information, the OTMF floods all the observation information throughout the network. A node can rely on the observation from neighbours (called second-hand information) for determining its own weights. The problem of the mechanism is the generation of a significant amount of overhead to MANETs. In [6, 35], the authors have mentioned about trust-related information extracted from the three layers of a networking system namely physical, core and application layers; and they use the information for quantifying trust. An inference engine based on fuzzy logic is used to infer a trust level. However, the drawback of this approach is only focusing on objective factors but not on subjective factors of trust. As a result, values they got from the computation mechanism do not reflect some key characteristics of trust, thus cannot be quantified as trust. An interesting article is about judging trust based on several features extracted from social interactions such as spatiality, relative orientation, frequency of interactions, and duration of interactions [36]. However, this information is not sufficient to accurately derive trust due to a variety of assumptions on relations between trust and behaviours of entities which are sometimes not correct.

Some trust models imitate the human cognitive process to form a belief value by considering several types of TIs such as reputation and recommendation and observation. These models have been proposed for trust evaluation and trust management in P2P networks [37], Social Networks [38], IoT [11, 39] and in SIoT [40]. Most of them are based on interactions among entities in (social) networks to evaluate trust, resulting in a distributed, activity-based or encounter-based computation model. Here, trust is derived only based on social concepts such as reputation, recommendation and experience by propagating knowledge among entities. Reputation has been widely used in many applications and e-Commerce websites such as eBay, Amazon, and IMDb, however, the biggest drawback of these reputation schemes is the requirement of human participants to give feedback on their opinions about the entities they have interacted with. In addition to the online transactions in e-Commerce, reputation schemes can be used in purely P2P, MANETs and WSNs systems that facilitate interactions among entities distributed over a network. For instance, many trust-based routing protocols in WSNs and MANETs assess trustworthiness of a node in the networks by considering third-party opinions and reputation as well as their own experiences based on their understanding to make sure that a node is not going to be misbehaved and compromised. Based on the trustworthiness value, a decision maker will choose whether the node is put into routing paths or not. For example, a time-sensitive and context-dependent trust scheme in MANET is proposed as a combination of self-measurement and neighbour sensing (as recommendation) for enhancing trust evaluation accuracy [41]. Nitti *et al.* in [40] have also proposed a trust management scheme in the IoT that incorporates several TIs extracted from feedbacks such as credibility, relationship factors, and transaction factors; as well as incorporating some TIs from direct knowledge such as computational capabilities showing the potentiality of an object to damage other objects.

Another notion of trust is ranks among webpages introduced by Google in their PageRank mechanism [42]. In this example, webpages are listed in descending order of levels of trust between a user and a webpage. The trust goal in this case is that the webpages should be the correct targets the user is searching for. The mechanism actually assesses a composite of reputation and importance of a webpage by observing network behaviours with an assumption that “the more back-links to a webpage, the more reputation and importance it gets (and higher probability users will visit such a webpage)”. In this sense, PageRank value is partial trustworthiness of a webpage and it is used as a TI. Even though PageRank is just a portion of trust and does not carry some important characteristics (e.g., subjectiveness and transitivity); in this webpage ranking scenario, it is effectively used on behalf of trust.

3.3 Trust Model and Evaluation Mechanisms

The trust model presented attempts to tie together all trust attributes. We attempt to capture the semantics of the trust relationship using a proposed trust model and design a trust ontology that serves as an upper level ontology for use across multiple domains. Using this trust ontology, we can ask questions like: What are the trust relationships that an agent is participating in? Is there a trust relationship between agent X and agent Y? What is the scope of a trust relationship? What process was used to arrive at this trust value? These questions are formulated as queries using the trust ontology in the next part.

In this part, the trust model needs to cover all aspects of the trust relationship. Following the general trust model above, we model the trust relationship between two agents as a six-tuple relationship trustor, type, scope, value, process, trustee (as shown in Figure 3-1). The trust relationship between two agents is represented as a six tuple. The agent who trusts another agent is called the trustor and the agent being trusted is called the trustee. Each trust relationship is further qualified with [43]:

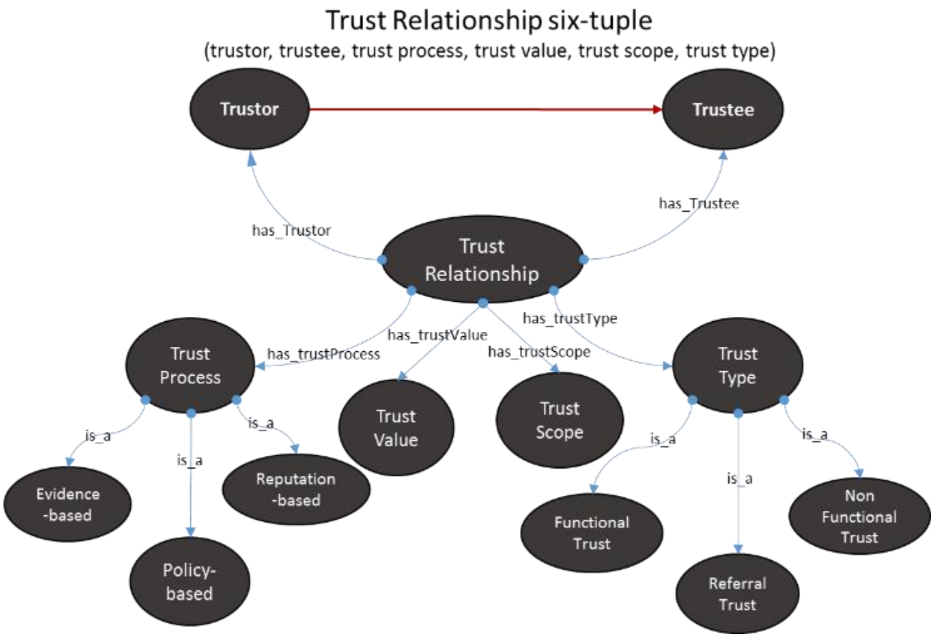


Figure 3-1. Trust Model illustrating all the concepts and relationships between the concepts

- **Trust Type:** The trust type captures the semantics of the trust relationship. Trust type can be functional, referral or non-functional.
    - Functional Trust: Trust relationship established with direct interactions between two agents. One agent trusts another agent's ability to carry out a particular task.

  - Referral Trust: Trust relationship established for conceiving an agent's referral of another agent. An agent trusts another agent's ability to recommend a third agent.
  - Non-Functional Trust: Distrust in agent's competence or behaviour established. Note that referral trust is transitive within the same scope, while functional trust is not.

- **Trust Scope:** Trust Scope captures the context in which the trust relationship is valid. A trust relationship is valid only in a prescribed scope. An agent that trusts another agent in one scope may distrust the same agent in another scope. For instance, an agent A can have functional trust in agent B for music and, at the same time, have non-functional trust in agent B for books.
- **Trust Value:** Trust value is a way to quantify or compare trust relationship. Value can be a natural number, real number in the range (-1, 1), or a partial ordering of trust relationships.
- **Trust Process:** The process by which we arrive at trust values is termed as Trust Process. The trust process will indicate the way in which trust values are computed and updated, essentially leading to trust management. This can include specific trust computation algorithms and application of specific techniques for trust computation, aggregation and management. Some examples of trust processes are described below:
  - Policy Based Trust: An agent trusts another agent based on some policy or rules. For instance, if a company is ISO 9001 certified, then we can expect a certain quality enforcement in the products they deliver.
  - Reputation Based Trust: If an agent has a record of previous interactions with another agent, then this can act as a basis for inferring trust and this is termed as reputation based trust process.
  - Evidence Based Trust: Evidence-based trust is the process of arriving at trust values by seeking additional confirmatory evidence for a known fact in order to validate or invalidate what is already known.

The idea of trust process is to abstract the method of arriving at trust values and managing them. There is no universal trust algorithm that fits all domains and applications. This abstraction will allow us to talk about trust across domains and use application specific or domain specific trust algorithms for each class of problems. Reputation based algorithms and entropy based algorithms are some examples of trust processes used within sensor networks. Trust evaluation enables trust modelling and reasoning about trust [44]. They are closely related to reputation systems. Simple forms of binary trust metrics can be found e.g. in PGP [45]. The first commercial forms of trust metrics in computer software were in applications like eBay's Feedback Rating. Slashdot introduced its notion of karma, earned for activities perceived to promote group effectiveness, an approach that has been very influential in later virtual communities.

3.4 Evidence-based and Policy-based Trust Evaluation Models

This approach has been intensively investigated in the previous decade (from 2000 to 2005) in which policies or rules are used in the trust computation. To establish and calculate trust, a trust management needs to integrate trust negotiation protocols for creating, exchanging and managing credentials of network entities. The policy-based trust methods generally assume that a trustor, after several processes of credential creation and exchange, will obtain a sufficient number of credentials from the trustee and from other entities for trust establishment and trust calculation. There is an issue called "recursive problem" which is related to the trust of the credentials in this approach. This problem can be solved by introducing a trusted authority (a third party entity) for issuing and verifying these credentials.

The policy-based trust mechanism is usually used in the context of distributed network systems as a solution for access control and authorization [46-49]. The goal is simple by judging whether a user is trustworthy or not based on a set of credentials and predefined rules before granting rights to access network resources. The focus in this situation is how to apply policy languages, entities ontology and reasoning engines for specifying and producing additional rules and trust knowledge for trust computation procedures.

For the summary research related to policy-based mechanisms, we organized the research work into sub-categories of trust computation procedures: trust credentials establishment, trust negotiation process, and policy/rules trust languages.

- **Trust Credentials Establishment:**
  Conventionally, credential is information about an entity and context of the environment needed to evaluate trust. Although the word "credential" is frequently used in many research works, there is no common definition or standard to specify and determine it. Policies should rely on credential information and other context properties in order to judge trust. An obvious example of credentials in trust is the use of username and password to gain access control when logging on to a computer. According to the system policy, having a correct username in accordance with an appropriate password proves that the user is trusted by that computer system. In a more complicated example, credentials are also automatically generated during a negotiation process by leveraging security certificates with digital signatures or using public key infrastructure (PKI). Note that only certificates that include trust-related information of an entity or context can be used as credentials. For example, TrustBuilder [50] dealt with trust by establishing trust credentials using traditional security techniques such as authentication and encryption which is called "hard security" trust.

A well-known research work related to credential exchange is the Kerberos protocol [51]. The protocol considers a user as the trustee and a computer as the trustor and enables them to securely exchange their own verifiable credentials. To do this, the Kerberos system needs to use a third party, in this case another computer, to facilitate the credentials exchange process. However, this approach is no longer used since the current network systems like the IoT are much more complex and are facing many intelligent attacks.

Recently, many researchers have considered “credentials” in a broader perspective and have used the term “trust metrics” and “technical attributes” instead of “credentials”. This approach allows us to develop trust to be more flexible, scalable and effective.

- **Trust Negotiation Process**

  An important issue when exchanging and generating credentials is the undesirable revealing of information to malicious entities, resulting in loss of security and privacy. The question raised is: To what extend an entity trusts other entities to see its own credential information in exchange for earning their credentials. There are many research works dealing with this trade-off between gaining trust and sacrificing privacy such as in [52-54]. These researchers considered several particular contexts in accordance with types of credentials and number of credentials. They analysed the loss of privacy once any credentials are revealed to other entities. This trade-off approach has motivated some researchers to develop a trust platform by developing architecture systems based on that trade-off principle.

  TrustBuilder is a typical example in which a mechanism is implemented for analysing and choosing the reasonable solution for the trade-off in the context of web services [50]. The trustor needs to understand the risk of losing privacy information when revealing credentials in exchange for earning trust. Based on this mechanism, trust is gained when a successful trade-off is made: sufficient credentials are revealed while privacy is still maintained in some level. The concept of trust transitivity property is also characterized in TrustBuilder in the form of “credentials chain”. For example, if entity A trusts B’s credentials, and B trusts C’s credentials, then A trust in the credentials of C in some degree.

  Based on the credentials chain concept, some research works designed and developed trust frameworks that perform credential chaining and credential exchange such as in PeerTrust [55], PROTUNE [49], RT10 [56].

- **Policy Languages and Trust Languages**

  Ontologies and Context-aware mechanisms are also soon introduced when developing credentials in the context of client-server system [57] and Semantic Web [58]. It is needed to design formalism for trust-related information, e.g., credentials and trust metrics in order to develop a trust system. This objective can be achieved by incorporating findings from logic to automate various kinds of reasoning, such as the application of rules and policies or the relations of sets and subsets for the Trust Computation process. Most researchers have used the Semantic Webs techniques such as semantic representation, policy languages, ontologies and reasoning mechanisms for the trust computation. The issue is how to represent and express trust information and trust knowledge. Some efforts have been made to create policy languages for trust as described in Table 3-1.

TABLE 3-1. COMPARISON ON POLICY AND TRUST LANGUAGES

Research Work	Network Environment	Trust Context	Policy/Trust Language Features
KAoS [59]	Distributed heterogeneous environments	Access Control for KAoS services	KAoS Policy language with ability of dynamic policy changes.
Rei [60]	Semantic Webs	For Security and Privacy Issues	Use semantic representation and model for dynamic policy manipulation. Allow each entity to set their own policy,
Global Computing [61]	Global Computing system	To replace key-based security	Include observation of trustee, recommendation from others and reference to other sources of the trustee. Use a formal policy language. Trust can be proved
WS-Trust [62]	Web services	Specification and OASIS standard providing extensions to WS-Security	Security Assertion Markup Language (SAML). Trust is gained through proofs of identity, authorization, and performance. To validate the security token.
[63]	Global Computing system, Dynamic Networks	For trust-based security mechanism	Policy language that use lattices of relative trust values. Allows fine-tuned control over trust decisions
Cassandra [64]	Large scale distributed systems	Role-based access control and Context-based system for authorization	Use a policy specification language based on Datalog with constrains with five special predicates. Trust is obtained after credentials exchanged.
[65]	Open Distributed System, WWW	Trust-based access control for web resources	Use ontology for representing trust negotiation policies. Rules are used to negotiate trust. Policies are more flexible than standard policy set, allowing simplification of policy specification
Policy Maker [66]	Distributed Systems	Trust-based authorization	Provide “proof of compliance” for request, credentials and policies. Allow individual systems to have different trust policies. PolicyMaker assertions can be written in any programming language.
KeyNote [67] [68]	Distributed Systems	Trust-based authorization	Same principles as PolicyMaker[66]: directly authorize actions (in accordance with credentials) instead of processing both authentication and access control.

			Require credentials and policies be written in a specific assertion language to work with KeyNote compliance checker.

3.5 Reputation-based Trust Evaluation Models

This approach uses history of interactions and behaviours among trustor, trustee and related entities, combines them in accordance with a reputation model in order to make a trust decision about the trustee. The history of interactions between trustor and trustee is sometimes called personal experience or direct reputation. The history of interactions between other entities and trustor is also called indirect reputation, referral reputation or recommendation.

There are many parallel research works on both reputation-based trust model and reputation model. The confusion between a reputation system and a trust system should be clarified. Trust and reputation are sometimes the same across multiple contexts or are treated as the same mechanism to support services. Basically, a reputation system collects feedback from entities after an interaction incurs. This feedback will be combined and calculated using several mathematical models to get a reputed score. This reputed score is sometimes misunderstood as trust level. Several reputation systems have been developed in the context of e-commerce systems and web services such as eBay [69] and Keynote [67, 68].These systems use a centralized authority to get ratings and feedback from users after each transaction and then update the overall reputed score by using several mathematical models as mentioned above. There are also some distributed approaches for reputation systems in which each entity establishes and maintains reputed scores to its neighbours by updating once any related interaction occurs by using several heuristic algorithms. It is required to integrate these scores due to the use of deterministic numbers for representing reputation.

Reputation-based trust systems can be considered as a step forward compared to reputation systems in which the trust computation mechanism combines not only ratings or feedback from entities but also trustor and trustee properties and preferences; and context information to calculate trust level. In this sense, the reputation system is a part of the trust system. There has been a large amount of effort to investigate the reputation-based trust model and to develop reputation-based trust systems in many types of network environment such as in distributed systems, P2P networks, sensor networks, and grids. There are also some research works to build a network of trust in which trust is established and maintained between any two entities over time, resulting in creating a “web of trust”.

- **Reputation-based Trust in Distributed System and P2P Networks**

The trust models in this part try to create a trust system that entities are able to establish, calculate trust level, and make trust decisions rather than relying on a centralized authority. The contribution in this approach is how to create appropriate credentials, TIs and TAs that are provided to each entity to produce trust. Depending on different purposes of applications in each network environment, reputation-based trust systems are utilized accordingly. For example, in distributed systems, many research works focus on the detection of malicious entities and prevention of network attacks while the trust system in P2P networks is to guarantee the quality of data transfer.

- **Reputation-based Web of Trust**

  Almost every effort in this idea uses the concept of credentials chain. The majority of trust evaluation transitivity has been focused on using reputation. In this scenario, each entity maintains reputation information on other entities, thus creating a "trust network" or "web of trust".

  There are two approaches for trust systems in the web of trust. The first approach assumes that trust credentials and TIs already exist, and the trust systems are trying to propagate these credentials and TIs among entities whose credential and TIs may not have been evaluated for trust. The latter supposes that a web of trust is given in which a link between two entities. It does not matter how these links are made as long as the trust can be quantified. If there is no link between two entities, it means no trust decision has been made, and trust transitivity should be applied in this scenario. The summary and comparisons of reputation-based trust computation in the above discussed perspectives are described in detailed in Table 3-2.

TABLE 3-2. FEATURES COMPARISONS AMONG REPUTATION-BASED TRUST MODELS

Research Work	Network Environment	Trust Context	Reputation-Related Features
[70, 71]	Distributed System	Malicious Node detection	Define Agent, Trust Relationships, Trust Value and Trust Categories. Define first-hand knowledge as direct reputation and second-hand knowledge as recommendation. Propose Recommendation protocol for trust propagation.
[72, 73] [74]	Distributed System Social Network	Reputation Management	Reputation information is obtained from external sources. Allow entities to actively determine trust using reputation information obtained from other entities. Avoid hard security by distributing reputation information allowing individuals to make trust decisions instead of a centralized trust management system. Weight the reputation information by the reputation of those sources for providing good information.
[75]	Social Networks Multi-agents system	Reputation System	Analyze the reputation information by characterizing the indirect and direct information. Considering the social relation in calculating reputation score. Put the context information into account.

[31]	Open Networks	Trust-based authentication	Provides methods for computing degrees of trust in the presence of conflicting information.
[76, 77]	P2P Networks	Reputation and Trust for Webpages ranking	Propose PageRank algorithm for ranking websites by authority. EigenTrust algorithm using PageRank to calculate global reputation value for each entity. Credentials for reputation in this work is the quality of a peer's uploads (e.g., did the file successfully upload?) within a peer-to-peer network.
	P2P Networks	Reputation System	Propose XRep protocol which allows for an automatic vote using user's feedback for the best host for a given resource.
[79, 80]	Web of Trust	TrustMail application	Use ontologies to express trust and reputation information, which then allows a quantification of trust for use in algorithms to make a trust decision about any two entities. Trust transitivity is considered as credentials chain. Local reputation and Global reputation is also taken into account.
[81, 82]	Web of Trust P2P Network	Trusted applications in Open Network	Define controversial users who are both trusted and distrusted in particular context. Globally computed trust value (in a web of trust) for a controversial user may not be as accurate as a locally computed value due to the global disagreement on trust for that user. Propose a method that performs a global computation on reputation values but considers the individual's input to the evaluation as the user preferences.

3.6 Hybrid Trust Evaluation and Trust Aggregation

Several research works have tried to combine both reputation, evidence and policy-based models as a hybrid trust model in order to take advantage of both approaches while maybe getting rid of their drawbacks. This idea has recently become more popular in the context of the IoT where trust is more complex because many factors contributed to the trust establishment and to the trust computation. In the IoT environment, history of interactions and behaviours of entities are not only for reputation information but also for trust-related knowledge extraction. The combination of reputation information, knowledge and relationships among entities in the IoT draws a very complicated picture of trust computation.

In the hybrid model, Reputation is considered as one of several TIs. The Reputation TI can be obtained by using the reputation mechanisms and reputation systems that have already been developed and mentioned above. That is the content of the Trust Aggregation procedure in which trust evidences (TAs, TIs) are collected through several techniques, such as self-observation or reputed information in the form of feedback and recommendations.

TIs can be gained from sufficient TAs by using trust aggregation techniques, for example, TIs can be computed by using Weighted Sum [83, 84], Fuzzy-based algorithms [85, 86], Belief Theory [87, 88], Bayesian mechanisms [89, 90]. The summary is described in Table 3-3. The trust aggregation techniques and reasoning mechanism are the crucial parts needed to investigate and develop in order to build a completed trust platform in the IoT.

TABLE 3-3. SUMMARY OF TRUST AGGREGATION TECHNIQUES

Aggregation Techniques	Research Work	Importance Technique Features
Weighted Sum	[83, 84]	Entities with a higher reputation or transaction relevance have a higher weight. Entities with strong relationships to trustor have higher weight. Use credibility as weight associated with indirect trust (recommendation or feedback). Use similarity as weight for indirect trust aggregation.
Fuzzy Logic-based	[85, 86]	Fuzzy Logic deals with reasoning that is approximate rather than fixed and exact. Fuzzy logic variables may have a truth value that ranges in degree between 0 and 1 and produce a partial trust where the truth value may range between completely true and completely false as trust levels. Linguistic variables are used as trust levels and managed by specific membership functions. Then trust is represented as a fuzzy measure with membership functions describing the degrees of trust (trust level).
Belief Theory	[87, 88]	Belief theory (evidence theory or Dempster-Shafer theory (DST)) deals with reasoning with uncertainty, with connections to other techniques such as probability, possibility and imprecise probability theories. Trust can leverage the subjective logic by operating on subjective beliefs about the network environment, and used opinion metric to denote the representation of a subjective belief. Used in trust computational model to compute trust of agents in autonomous systems by modelling the trust by belief, disbelief and uncertainty of an entity to other entities. It makes use of a base rate probability in the absence of evidence. The average trust then can be calculated as the probability expectation value between trustor and trustee. Subjective logic operators such as the discount and consensus operators can be used to combine opinions (self-observations or recommendations).
Bayesian Methods	[89, 90]	Trust can be considered as Bayesian interference: a random variable following a probability distribution with its model parameters being updated upon new observations. Can be used as a trust computational model because of its simplicity and sound statistical basis. Trust value can be modelled as a random variable in the range of [0, 1] following Beta distribution in which Belief discounting can be applied to defend against malicious entities such as bad-mouthing attacks or ballot-stuffing attacks.

3.7 Research Gap

There are two conventional types of trust models: policy-based approach (or rule-based approach) and reputation-based approach. These two trust models have been investigated under the context of different network environments including the IoT with different purposes and goals. Traditionally, policy mechanisms manage the decision of a system by describing a pre-defined set of conditions (rules) and specific set of actions in accordance with each condition. In this manner, policy can assist in making decisions for trust computation when a certain ambiguity level occurs while assessing trust. As a result, policy-based trust models normally involve the exchange or verification of trust-related credentials called the trust negotiation process. A reputation-based trust model is basically used in trust computation for assessing trust score or trust level based on the history of interactions of related entities. The reputation information in this scenario could be either directly with the evaluator (direct reputation) or as recommendation by other entities (indirect reputation, recommendation or third-party information). The trust model based on a certain level of reputation information is obvious since it happens in the process when people analyse and examine trust.

In recent years, most researchers have accepted that reputation is one important factor of trust resulting in the dominance of reputation-based trust models compared to policy-based models. However, the gap is that there is no emerging solutions to integrate both approaches in their trust models in order to leverage the advantages of them. Also, there is no concrete and standard evaluation mechanisms for the Reputation as well as mechanisms for aggregating the reputation with other trust-related information such as trust credentials and recommendations. Nevertheless, both credentials and reputations are the important information involving in the trust transitivity among entities; and each of them has its own pros and cons that have motivated researchers to work on.

Therefore, to fill in the gap, there is a need to investigate trust evaluation mechanisms needs to be created in order to evaluate opinions of an entity towards another after each interaction; and to spread the opinions to others (in the form of feedback and recommendations). Moreover, there is a final step is to aggregate the set of the third-party information to finalize an overall score which is the reputation of a trustee. Again, the reputation is used for quantifying trust. Reputation, which is an indicator of trust, should not be confused with trust but partially affects trust. Therefore, each of the previous research works is as a separated piece of a big picture solving a particular challenge in a specific environment.

In order to synthesize such trust-related information, a trust aggregation method with a reasoning mechanism should be considered. It needs to be noted that the trust aggregation is a dynamic process which heavily depends on context-aware information, service requirements and trustor's preferences. Each trustor needs appropriate trust data, context data and aggregation methods for producing the desired overall trust score which reflects the trustor’s perspective and context awareness. Specific trustors might use and define different trust aggregation techniques for dealing with their associated trust data. There is currently no complete trust aggregation mechanism that can deal with the personalized trust in a dynamic context-awareness environment, however, several researchers have proposed some solutions for particular contexts and services

To summarize, in order to provide trust among entities in the IoT environment, research on trust evaluation should fill the current gap to achieve some goals in accordance with the deployment of a trust platform in the IoT system model.

Environment and scenarios in which a trust evaluation platform will be deployed. Based on this, trust model and evaluation mechanisms are characterized, developed and implemented.

A Trust Model and conceptual evaluation technique: a trust model in accordance with TIs and TAs. This task should specify TIs, TAs and environment characteristics and properties contributing to the evaluation process such as network characteristics and social relationships.

Trust Evaluation mechanisms and aggregation techniques: methods to examine the necessary TAs, TIs and overall trust value by aggregating such TAs and TIs.

3.8 Chapter Summary

In this chapter, an extensive range of trust computation mechanisms has been discussed. However, the current research methods are only focused on specific contexts and hence lack completeness. Therefore, a single unique solution is not presented for the trust computation and acquisition. Thus, issues are still open for investigation and some of the ideas are discussed here. Based in many papers that have been analysed above, there are many gaps that needed to be filled in order to have a complete trust understanding and development.

CHAPTER 4. TRUST CONCEPT, CONCEPTUAL MODEL AND REK EVALUATION MODEL IN THE IOT

4.1 Introduction

Trust is a complicated concept which was originally used in many disciplines in human life. In the IoT environment, trust interplays between social sciences and computer science influenced by both objective and subjective factors from both participants and contextual characteristics [91]. Trust can be roughly defined as "assurance" or "confidence" of a trustor in a trustee to perform a task in a way that satisfies the trustor's expectation. In this sense, the trustor partly recognizes the vulnerabilities and potential risks when the trustee accomplishes the task, thus it represents the trustor's willingness to be vulnerable under the conditions of risks and interdependence [92].

It is a critical factor that highly influences the likelihood of entities to interact and transact in both real-world and the digital world. Trust is crucial that it affects the appetite of an entity to use services or products offered by another entity. This example can be seen in our everyday life where trust decisions are made. When purchasing a product, we may favour certain brands or certain models due to our trust that they will provide better quality compared to others. This trust may come from our experience of using these brands' products (termed "belief") or from their reputations that are perceived from people who bought items and left their opinions about those products (termed "reputation"), or from suggestions of your surrounding network such as families and friends (termed "recommendation"). Similarly, trust also affects the decision of an entity to transact with other entity in the ICT environment. Both consumers and providers should trust each other before decisions to consume or to provide the services are made; otherwise fraudulent transactions may occur.

This section presents a novel trust concept, a conceptual evaluation model along with several potential evaluation mechanisms for various TAs including Social Trust, System Dependability (in the Knowledge TI), as well as the two TIs, Reputation and Experience.

4.2 Concept of Trust in the IoT

The earliest variants of trust in computer science are system security and data security that cover concepts of hardware, software and communications. A system is trustworthy if it is secure and not compromised, meaning that it identifies people accessing the system and only allows authorized users; and the data security ensures that data is only accessed by those authorized users even in the presence of adversaries. More than three decades ago, Thomson mentioned trust in his Turing Award lecture when writing a Unix program to be free of Trojan horses [93]. Security gets more complex in networked worlds such as the Internet and the IoT due to the increasing number of participants in systems throughout the networks, resulting in introducing more threats, vulnerability and risks. System security and data security are also more complicated when privacy is taken into account. For example, personal data security could be ensured (in some degree) but providers can use the data for their own purposes or sell to a third-party. In this case, data security might be compromised if the data owner's intent for data usage is violated. One of the solutions is a trust-based access control mechanism for data sharing in the environment of Smart City that we have proposed in [94].

An advanced variant of trust for a computer system is dependability that is evolved from reliability, security and privacy considerations. Besides security and privacy, reliability is a factor showing whether a system is going to perform properly. Thus, dependability is de facto a property of a system representing ability of the system to deliver secure and quality services by characterizing the security, privacy and reliability schemes in terms of some attributes such as availability, safety, integrity, confidentiality and reliability. Grandison and Sloman have defined this variant of trust as "infrastructure trust" [95]. In our perspective, dependability is one of the most important indicators in evaluating the trustee's trustworthiness (in case the trustee is a computer system). The key distinction between trust and dependability is due to the enrolment of social interactions (of both humans and devices), which is modulated in the form of social capital factors (Figure 4-1a). The social capital can interpret various aspects of individuals and social networks including behaviours, norms and patterns that have built up through social interactions over time that also help to compute trust. In this regard, trust is an umbrella concept of dependability.

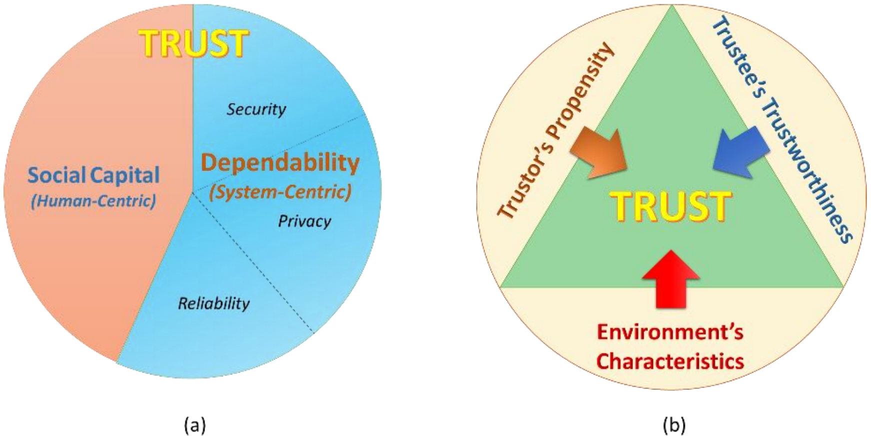


Figure 4-1. (a) Trust concept in the relation with dependability and social capital; (b) Three main aspects of trust in the IoT environment.

Trust is originally a foundational aspect of human social relations; and when applying trust to the IoT environment, it should be considered under a perspective of a trustor in correlation with a society. Social interactions, subjective viewpoint of individual entity, and environments should not be neglected [96]. We have pointed out that besides trustworthiness of a trustee, the trustor's propensity and environmental factors such as vulnerabilities, threats and risks also contribute to the trust evaluation (Figure 4-1b). This is obvious because trust only occurs in risky scenarios in which the trustor is going to be under vulnerability.

4.2.1 Definition of Trust in the IoT

A general definition of trust in computer science has been broadly acknowledged as follows:

Trust is defined as a belief of a trustor in a trustee that the trustee will provide or accomplish a trust goal as trustor's expectation within a specific context for a specific period of time.

Trust reflects the belief of a trustor in a trustee to dependably perform required tasks in a trust context as the trustor's expectation in the CPSS infrastructure. Thus, evaluation of trust requires to consolidate component analysis of networking systems in order to gauge where risks are incurred; in the meantime, it synthesizes with human interactions in the social domain as illustrated in Figure 4-2. Different trustors, trustees and trust contexts may have different business priorities, experience, opinions, threats, vulnerabilities, and risks resulting in different trust values.

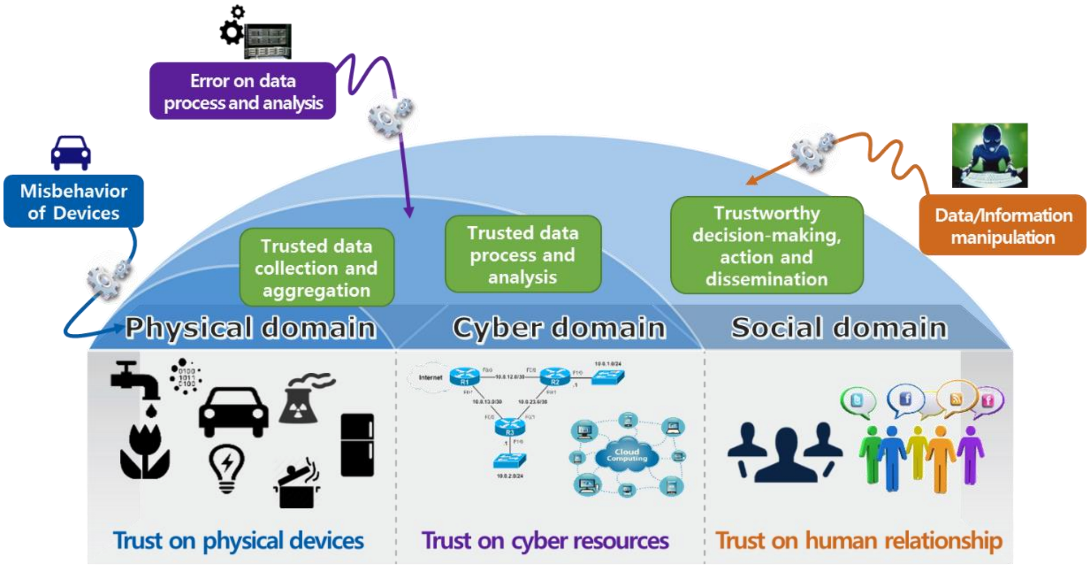

Error on data process and analysis
Misbehavior of Devices
Data/Information manipulation
Trusted data collection and aggregation
Trusted data process and analysis
Trustworthy decision-making, action and dissemination
Physical domain
Cyber domain
Social domain
Cloud Computing
Trust on physical devices
Trust on cyber resources
Trust on human relationship

Figure 4-2. Trust is estimated across CPSS

In IoT environment, trustors and trustees can be humans, devices, systems, applications and services. Measurement of trust as the belief (called trust value) can be absolute (e.g., probability) or relative (e.g., level of trust). The trust goal is in a broad understanding. It could be an action that the trustee is going to perform (trust for action); it could also be information that the trustee provides (trust for information). Trustor's expectations are deliberately considered to include specific requirements for performing well (in some degree) the trust goal. All of the terms in this definition will be described and explained in detail in the next sections.

4.2.2 A Novel Conceptual Trust Model in the IoT

It is important to clarify that trust is neither a property of a trustor (e.g., trustor’s preferences) nor a property of a trustee (e.g., trustee’s trustworthiness and trustee’s reputation). It is a relationship between the trustor and the trustee that is subjective and asymmetric which is derived from the triad of trustee’s trustworthiness, trustor’s propensity and environment’s characteristics. Based on the clarification of the trust concept, a conceptual trust model in the IoT is proposed as illustrated in Figure 4-3. Then, a more specific trust definition in the IoT associated with the conceptual trust model is proposed as follows:

Trust is the perception of a trustor on trustee’s trustworthiness under a particular environment (within a period of time) so-called perceived trustworthiness.

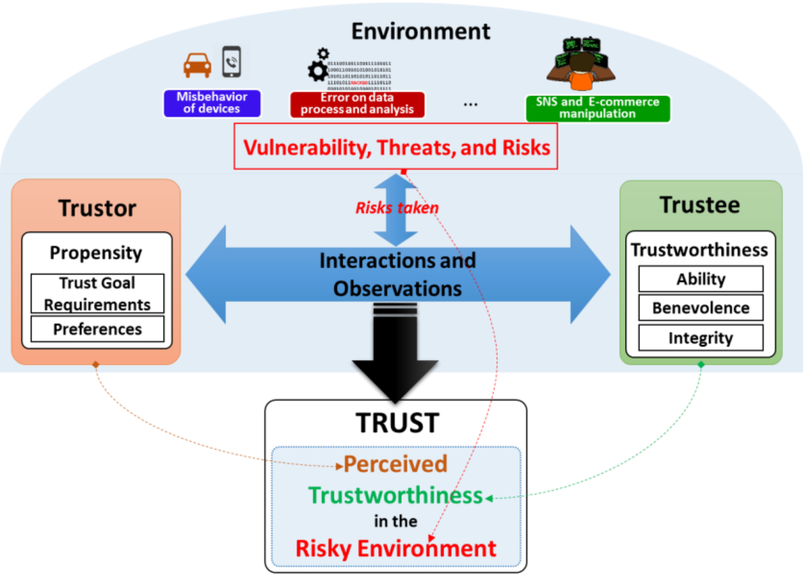


Figure 4-3. Conceptual Trust Model in the IoT environment.

According to the proposed model illustrated in Figure 4-3, trust will be obtained by harmonizing the trustor’s propensity and environment conditions into the trustee’s trustworthiness. The harmonization is accomplished by aggregating both the observation of a trustor toward a trustee and the interactions between the two. It is worth noting that the environment conditions are reflected as risks taken during the observations and interactions. The trustor’s propensity includes both requirements for the trust goal and the trustor’s preferences about the trustee’s trustworthiness whereas the environment conditions are the considerations for some factors such as vulnerabilities, threats and risks. The trust goal requirements with the environmental factors helps determining the set of TAs for deriving the perceived trustworthiness whereas the trustor’s preference is to help combining these TAs to obtain an overall trust value for making a decision. For example, trustor’s preferences could be represented in the form of weights of TAs, indicating the levels of importance of the TAs when constructing trust. Trust as perceived trustworthiness is an instance of a trustee’s trustworthiness with respect to a particular trustor and an environment, thus, even for the same trustee in the same environment, different trustors might have different propensities of the trustee's trustworthiness. This illustrates the subjective characteristic of trust. Another important characteristic of trust is the context-dependence that can also be illustrated using this conceptual model as follows: with the same trustor and trustee, different environments might result in different TAs and different trustors' propensities.

Based on the conceptual model, the goal of any trust model is two-fold: (i) to specify and evaluate TAs of the trustworthiness of a trustee with respect to the trustor's propensity and the environment conditions; (ii) to combine the TAs to finalize the perceived trustworthiness as the trust value. From now on in this article, the term "trust" refers to this conceptual model and it is interchangeably used with the term "perceived trustworthiness".

4.3 Trustworthiness and Trustworthiness Attributes

According to the proposed conceptual trust model, in order to quantify trust, it is necessary to investigate a trustee's trustworthiness by specifying TAs associated with it. As mentioned above, trustworthiness is a composite of a variety of TAs that illustrate different characteristics of the trustee. Despite a large number of TAs having been figured out in trust-related literature, TAs mostly fall into three categories as the three main dimensions of trustworthiness: Ability, Benevolence and Integrity. This classification is well-known and widely-accepted in the field of social organization settings [97]; and we believe it is also appropriate for consideration of trustworthiness in the IoT environment.

- **Ability**: is a dimension of trustworthiness showing the capability of a trustee to accomplish a trust goal. An entity may be highly benevolent and have great integrity for fulfilling a trust goal but the results may not be satisfactory if it is not capable. This term incorporates some other terms that have been used as TAs in much of the trust-related literature such as competence, expertness, and credibility.
- **Benevolence**: is a dimension of trustworthiness showing to what extent a trustee is willing to do good things or not harm the trustor. Benevolence ensures that the trustee will have good intentions toward the trustor. This term incorporates some TAs such as credibility, relevance, and assurance as TAs.
- **Integrity**: is a dimension of trustworthiness showing the trustee adheres to a set of principles that helps the trustor believe that the trustee is not harmful and will not betray what it has committed to do. These principles can come from various sources such as fairness, or morality. This term incorporates some TAs such as honesty, completeness, and consistency.

Table 4-1 lists a miscellany of TAs keywords classified into the three categories. Some of the TAs in the table are frequently used in trust literature ranging from social science to computer science, the others are rarely used and only exist in specific contexts. Even though each of the three factors Ability, Benevolence and Integrity captures some unique elements of trustworthiness, many of these keywords are not necessarily separated, and the interpretations of them clearly depend on particular environments and trust goals. For some specific environments and goals, certain TAs are similar whereas they are different in other contexts.

TABLE 4-1. SOME KEYWORDS OF TRUSTWORTHINESS FROM TRUST-RELATED LITERATURES CLASSIFIED INTO THREE DIMENSIONS.

Ability TAs	Benevolence TAs	Integrity TAs
Competence, ability, capability, expertness, credibility, predictability, timeliness, robustness, safety, stability, scalability, reliability, dependability	Good intention, goodness, certainty, cooperation, cooperativeness, loyalty, openness, caring, receptivity, assurance	Honesty, morality, completeness, consistency, accuracy, certainty, availability, responsiveness, faith, discreetness, fairness, promise fulfilment, persistence, responsibility, tactfulness, sincerity, value congeniality, accessibility

4.4 Trust Evaluation versus Risk Management

Apart from the main content of the chapter, it is worth mentioning the correlation between trust evaluation and risk management due to the need for assessing risk (in some degree) as environmental factors when evaluating trust. Managing risk for a computer system is a complex and multifaceted process including: (i) frame risk; (ii) assess risk; (iii) respond to risk once determined; and (iv) monitor risk. These four tasks require a full investigation of vulnerabilities, threats and risks in networking systems [98].

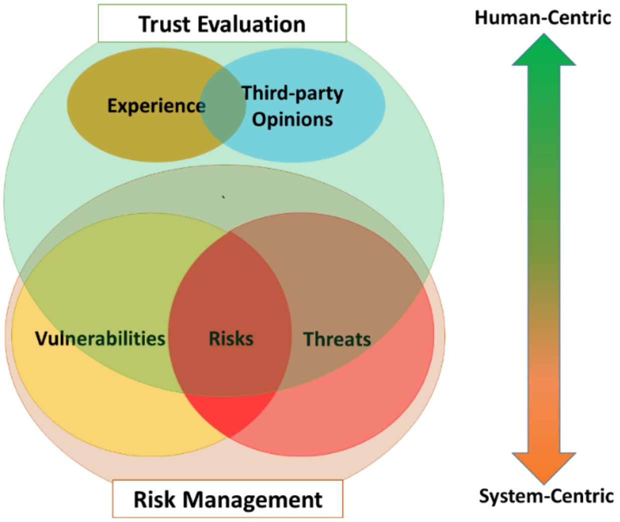


Figure 4-4. Trust evaluation and risk management in comparison.

The analysis of vulnerabilities, threats, and risks is also required in the trust evaluation but it is not necessarily fully involved in the risk management. Instead, trust evaluation takes social-related factors (i.e., Experience and Third-party Opinions) into account when judging trust (Figure 4-4). Risk management assesses an entity (i.e., a computer system) from the perspective of a system (system-centric) while trust considers the entity (the trustee) from the perspective of a trustor, expressing a subjective view of the trustor on the trustee in an associated social context (human-centric).

4.5 Conceptual Trust Evaluation Model

Trust can only be measured partly. It is impossible to measure trust completely due to a huge range of factors from both participants and environment contributing to the trust relationship. Moreover, some of them are unable to obtain or present a great challenge to measure.

As implied in the conceptual model in Section 4.2.2, a simple trust evaluation scheme could be as the following procedure: (i) determine and calculate all TAs of a trustee's trustworthiness; (ii) specify task requirements and preferences, (iii) figure out all environment conditions; then (iv) incorporate these factors to build trust. This trust evaluation model is called direct trust that indeed calculates trust based on direct observations of both the participants (the trustor and the trustee) and the environment. However, this approach finds it unfeasible to efficiently measure trust for several reasons. For example, there are a variety of TAs (some of them are listed in Table 1) which need to be quantified in order to measure the direct trust; and this is an impossible mission. One reason for this is due to the ambiguity and variability of natural language when defining terms for TAs that are still debatable in trust literature. Another reason is the complication and limitation of data collection, technologies and methodologies for valuating all the TAs as well as the complexity of incorporating TAs with a trustor's propensity and environment conditions to evaluate trust. Authors in [99] also mentioned that TA collection might cause privacy leakage which makes involved entities reluctant to provide personal evidence for a trust evaluation platform.

Consequently, instead of measuring trust using only the direct trust approach, a prospective approach is to determine a set of indicators called Trust Indicators (TIs) that are feasible, not so complicated to obtain, and cover different aspects of trust. As the word "indicator" implies, each TI is as a "piece of a puzzle" showing the consensus of trust. TIs could be a TA or a combination of several TAs; could also be a combination of some TAs with the trustor's propensity and environmental factors. TIs can be obtained using different approaches, for instance, the direct trust evaluation model could produce a good TI. However, other TIs do not necessarily only stick to the direct trust evaluation scheme. Thanks to the integration of social networks, some TIs can be determined based on social interactions in the IoT environment that effectively indicate trust such as Recommendation and Reputation which are evaluated contingent on the propagation characteristic of trust. These TIs are then combined to derive a portion of the complete trust called computational trust. The computational trust is persuasively used on behalf of the complete trust (Figure 4-5). As many TIs are specified and evaluated, the more accurate the computational trust will get. However, as two sides of a coin, there is always a trade-off between computational trust accuracy and computational efforts.

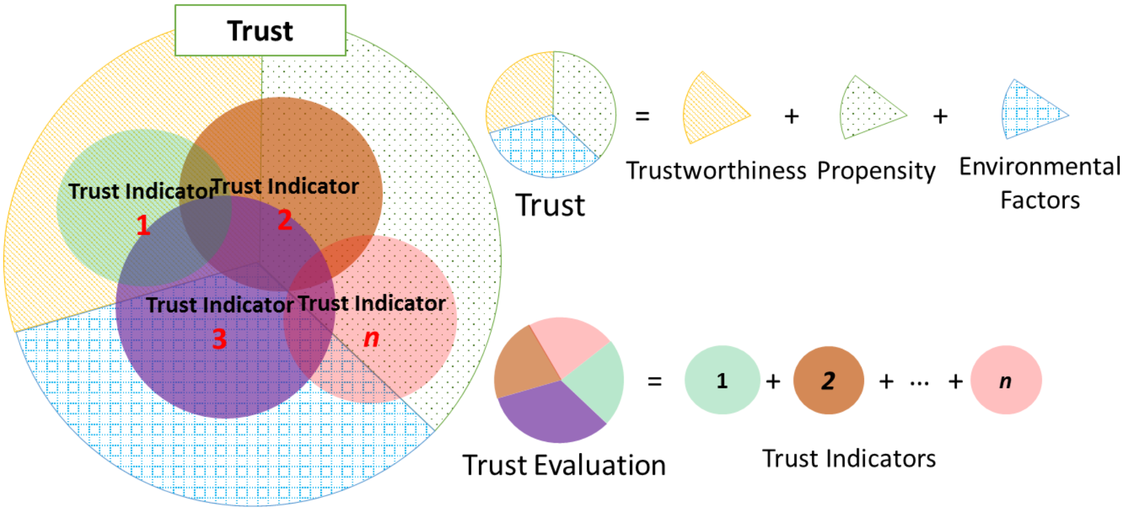


Figure 4-5. Concept of computational trust that is comprised of multiple trust indicators.

Nevertheless, any trust evaluation models in the IoT environment should determine two objectives: (i) specify a set of TIs in which each TI represents a piece of the three factors: trustee's trustworthiness, the trustor's propensity, and the environmental factor; (ii) propose mechanisms to evaluate the TIs as well as to derive the computational trust value from the TIs. Again, the computational trust should be much similar to the complete trust so that it can be efficiently used on behalf of the complete trust in most of the cases.

4.6 REK Trust Evaluation Model

We propose a trust evaluation model that comprises a triad of Reputation, Experience and Knowledge TIs so-called REK Trust Evaluation Model (Figure 4-6). The reason to come up with the three TIs is that in social science, people normally base their determination of trust on three main sources: (i) public opinion on a trustee (as Reputation); (ii) previous transaction with a trustee (as Experience); and (iii) understandings of a trustee (as Knowledge). We believe this social cognitive process could be applied to the IoT environment.

As depicted in Figure 2-1, trust is comprised of three TIs called Reputation, Experience and Knowledge. Knowledge is as "direct trust" and evaluated by inferring trustees' characteristics considering the trust context[100].

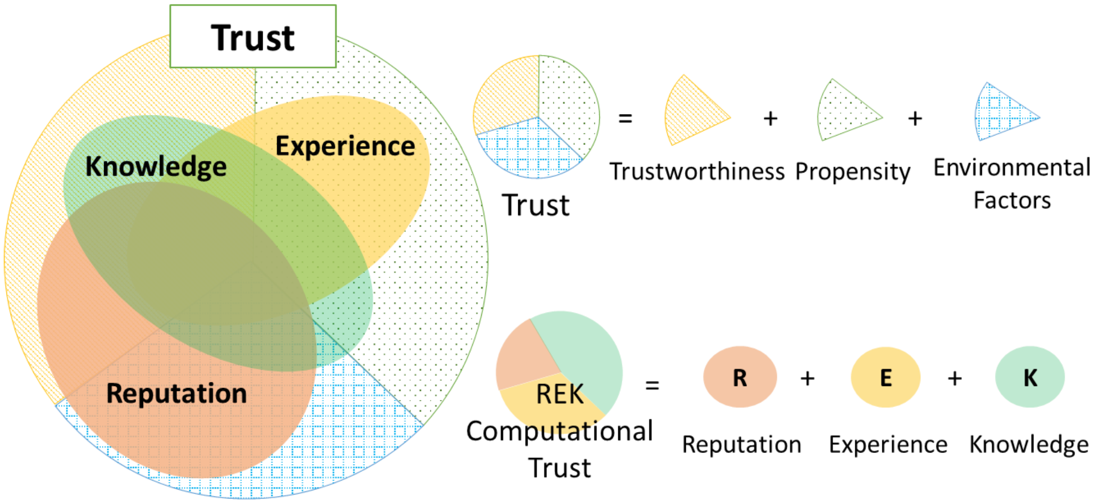


Figure 4-6. Reputation, experience and knowledge as the three indicators in the REK trust evaluation model.

Knowledge TI is the direct trust that renders a trustor's perspective on a trustee's trustworthiness in a respective environment. Knowledge TI can be obtained based on limited available information about characteristics of the trustee and the environment under the trustor's observation. Knowledge TI can reveal a portion of trust which is illustrated in Figure 4-6. It indicates more about trustworthiness of the trustee and trustor's propensity but not much about the environmental vulnerabilities, threats and risks. Experience and Reputation TIs are social features and attained by accumulating previous interactions among entities in the IoT over time. Experience TI is a personal perception of the trustee's trustworthiness by analysing previous interactions from a specific trustor to a particular trustee in various contexts. As the personal perception, Experience TI indicates more about a trustor's propensity but not a trustee's trustworthiness and environmental factors due to limited knowledge obtained. Reputation TI, instead, reflects global perception about a trustee by aggregating all previous experiences from entities (in a society) with this trustee. Thus, Reputation TI is able to effectively exhibit the trustee's trustworthiness and the environment characteristics; but not the trustor's propensity (Figure 2-1).

In IoT scenarios with billions of entities, there is a very high possibility that there are no prior interactions between two any entities, resulting in no Experience. Therefore, Reputation TI is a necessary indicator for trust, especially in the case where there are no previous interactions between a trustor and a trustee. Reputation is taken into account when evaluating trust because of the propagation characteristic of trust: each entity (a trustor) which has previous interactions with a specific entity (as the trustee) has its own opinions; and a reputation model (or a recommendation model) lets it share the opinions (as its recommendations) to others. Entities, then, can refer the opinions as one of the cues of trust to personally judge trust. By doing so, trust is propagated throughout the network. By synthesizing the three TIs, the REK Trust Evaluation Model consolidates the computational trust so that it can be used on behalf of the complete trust in most cases in the IoT environment with high accuracy.

- **Knowledge TI**

  Knowledge TI consists of two major sub-TIs called Social Trust and System Dependability.

  - **Social Trust sub-TI:** For the Social Trust, the four attributes namely Similarity, Honesty, Community-Interest, and Cooperativeness are taken into account [Figure 4-7]. These four factors are chosen to determine whether the service provider is a malicious entity; and also to prevent various type of social attacks in social networks such as self-promoting, bad mouthing, and ballot stuffing [101]. Consequently, the Knowledge TI covers all aspects of the direct trust to guarantee that the metric precisely indicates how well the trustee accomplishes the given task. Most TAs under the dependability sub-TI have been already figured out based on properties of the CPS environment. Depending on particular trustor, trustee and trust context, these TAs are obtained using different models with different computation methods. In some cases, several TAs might be simplified or are not necessary to evaluate. The TAs under the social trust sub-TI are still under investigation. All of them are derived from a trustee's relationship and social behaviour in the social domain of the ecosystems.

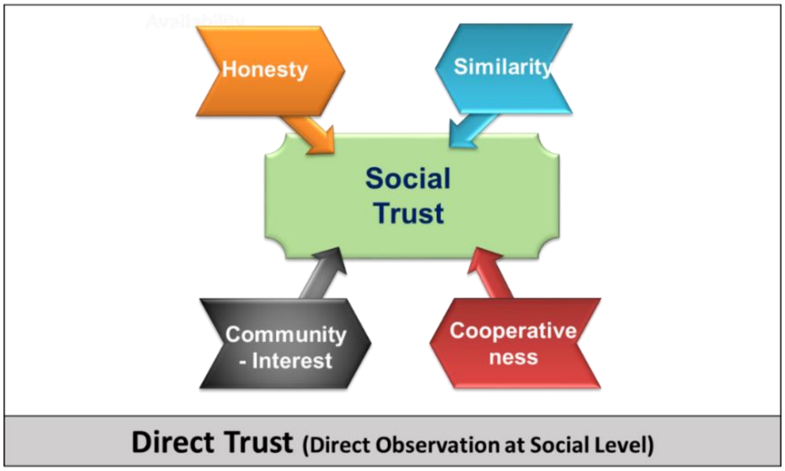


Figure 4-7. Four Components as the aspects of the Direct Observation at Social Level of the Social Trust

  - **System Dependability**: System Dependability renders the trustor's understanding of a trustee throughout the Physical and Cyber layers as a part of direct observation that is related to system level. The catalyst for the observation is to assess whether the trustee operates according to expectations or not. Therefore, the six factors (i.e., Availability, Confidentiality, Integrity, Safety, Reliability and Serviceability) in the two layers (Physical and Cyber) are taken into account as six TAs (Figure 4-8).

Consequently, the System Dependability sub-TI covers all aspects of direct trust to guarantee that this metric precisely indicates the ability of the system - which the trustee is based on, to dependably accomplish a given task. The six TAs are evolved from several attributes; and are quantitatively or qualitatively measured based on different types of information and methodologies which have been intensively explored over time [102].

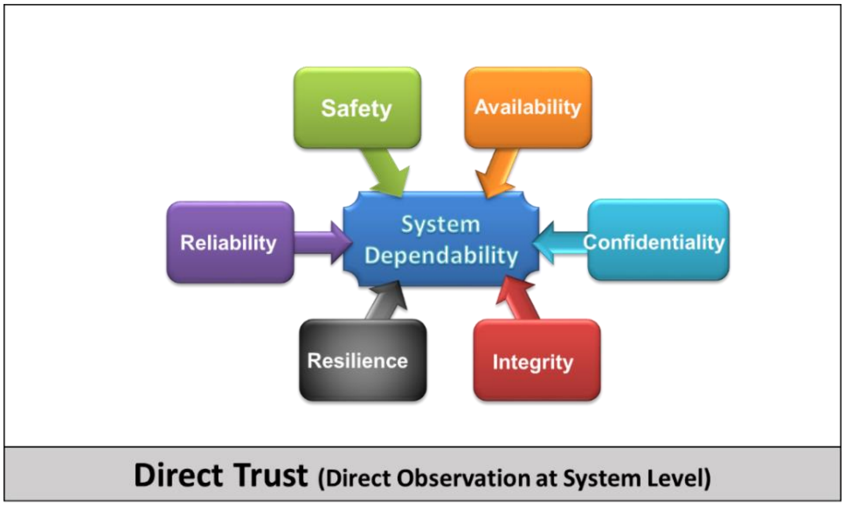


Figure 4-8. Six Attributes of the System Dependability sub-TI

- **Experience TI**

  The Experience TI is obtained by accumulating interactions among entities in the IoT over time. The Experience TI is a personal observation considering only interactions from a trustor to a trustee whereas the Reputation TI reflects the global opinion of the trustee. Interactions can be defined in several types of information between a trustor and a trustee. For instance, interactions might be feedback from consumers after each transaction (as used in many e-commerce systems), might just be a Boolean value (0/1) indicating whether a service transaction successfully operates or not (as in some reputation-based trust systems), or might be a hyperlink indicating the connection between two webpages (as in PageRank [42]). Figure 4-9 illustrates how Experience TI is formed between two entities based on previous interactions between the two.

- **Reputation TI**

  Reputation is the trustor's public assessment regarding the trustee's prior behaviour and performance. Reputation can be evaluated based on accumulated experiences of trustors about the trustee as shown in the right hand side of Figure 4-9. To acquire trust information based on the reputation of a trustee, two kinds of information are necessary to examine: (i) the previous trust transactions from all entities to the trustee; and (ii) the relationship between the trustor to the trustee.

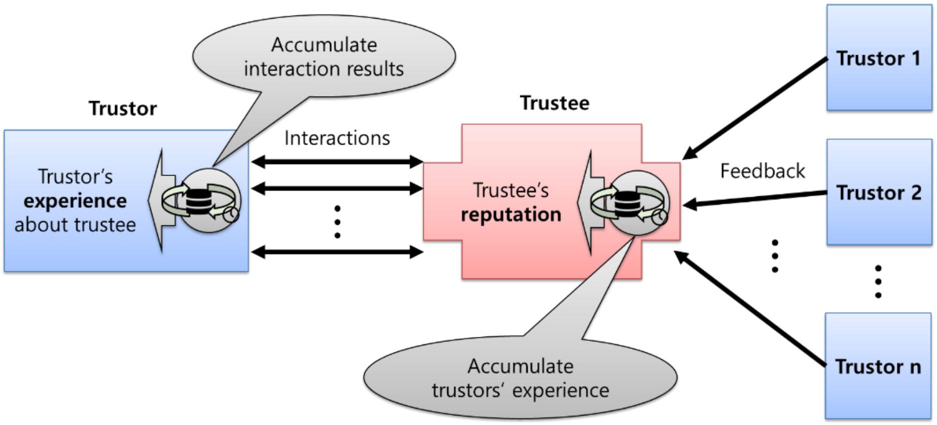


Figure 4-9. Indirect trust (Experience and Reputation)

We have investigated several reputation models for evaluating, propagating and managing trust in both centralized and distributed system architecture. We have come up with a semi-approach for our trust platform architecture that leverages Fog computing as a prospective solution [103]. A Fog component called Trust Agent is integrated in the IoT infrastructure to collect trust-related information, to store, and to process some simple calculations on trust for a local network in large-scale distributed systems like the IoT. The Experience TI can be calculated here by using a simple weighted sum or a heuristic algorithm as used in many centralized reputation authorities such as eBay and IMDb.

For obtaining the Reputation TI of a trustee, two kinds of information are necessary to examine: (i) the previous trust transactions from all entities to the trustee; and (ii) the social relationship between a trustor and the trustee. The authors in [104] have come up with a non-biased PageRank-like mechanism for calculating reputation values of trust for all entities in a distributed network. The mechanism, however, is conducted in a centralized authority (residing in a Fog controller) since it requires to aggregate necessary information on trust transactions from Trust Agents, Trust Brokers, and the relationship graph of the whole network. Consequently, a new network indicating the accumulated trust values for all entities is generated.

4.7 Chapter Summary

In this chapter, we have provided a comprehensive understanding of the trust concept along with a novel definition of trust in the IoT environment, considering three main factors influencing trust called Trustor's propensity, Trustee's trustworthiness and Environment's characteristics. Based on the clarification of trust in the IoT, a conceptual evaluation model is proposed accordingly which introduces the concept of TIs, respecting the trilogy: trustor's propensity, trustee's trustworthiness and environment's characteristics.

The chapter also introduced the REK evaluation model, leveraging the conceptual evaluation model, which specifies Reputation, Experience and Knowledge as the three major TIs which consider multi-dimensional trust aspects from direct observation to third-party information. In this chapter, necessary TAs, for covering the direct observation of trustworthiness as the Knowledge TI considering the three dimensions Ability, Benevolence and Integrity of any entities in the IoT environment, are also examined. Also, the conceptual evaluation model for the Experience and Reputation TIs leveraging the sociological behaviours of human in the real world are introduced.

CHAPTER 5. REK TRUST EVALUATION MECHANISMS

5.1 Introduction

In this chapter, we present and describe evaluation mechanisms for the three TIs Reputation, Experience and Knowledge in the proposed REK trust evaluation model in detail.

Knowledge TI unfolds perception of a trustor toward a trustee about how trustfully it accomplishes a trust goal in a specific context in the IoT. It leverages the direct trust evaluation model, thus, comprising of two major tasks: (i) specify a set of TAs for the trustee's trustworthiness that reflects the trustor's propensity and the environmental factors; and (ii) an aggregation mechanism to combine these TAs for deriving the direct trust as the Knowledge TI value.

Experience is a social concept that represents personal understandings and opinions about one entity to another based on its previous interactions with the counterpart. Reputation is a social concept which corresponds to a general understanding about an entity's characteristics. Reputation systems have been intensively explored in both computer sciences and information sciences in the last two decades [122-125]. The primary goal of a reputation system is to accurately provide information about the trustworthiness of an entity (as a trustee) to others (as trustors), thus, encouraging the trustors to participate in online transactions without first-hand knowledge. Most reputation systems are based on a feedback mechanism for managing opinions of participants after transactions, in both positive and negative forms. The difference between Experience TI and Reputation TI in the trust perspective is that Experience is a subjective relationship from a trustor to a trustee by considering interactions from the trustor to the trustee; whereas Reputation is an objective property of the trustee by considering interactions from all entities to the trustee.

5.2 Knowledge Trust Indication

In this section, a general TAs set is introduced which covers sufficient information to evaluate direct trust in the IoT environment; then, a TAs set for a specific use-case is specified and described later in Chapter 6.

5.2.1. Trust Attributes in Knowledge TI

We specify six important attributes introduced in the system dependability concept namely Serviceability, Safety, Reliability, Confidentiality, Availability, and Integrity as six TAs for the Ability dimension of the trustworthiness illustrated as D1 to D6 in Figure 5-1 and are described in details in Table 5-1. These six TAs could precisely indicate the capability of a trustee to dependably accomplish a trust goal. Besides, the Ability dimension might contain other TAs according to a specific scenario. For instance, in the User Recruitment in the MCS use-case, the spatial distance between a trustor and a trustee is considered as a TA. The meanings of the six TAs in quantifying trustworthiness are as following:

- **Availability**: Probability of an entity in operation in a given period of time.
- **Confidentiality**: Preserving the authorized restriction on access and disclosure on data, information or system.
- **Integrity**: Ability to guard against improper modifications and destruction.
- **Safety**: A property to guarantee that an entity will not fail in a manner that would cause a great amount damage in a period of time.
- **Reliability**: Probability that a component correctly performs a required job in a specified period of time under stated conditions.
- **Serviceability**: Property indicating how easily and simply a system can be repaired or maintained.

Generally, combination of the TAs is a measure of a system's capability to accomplish a given task that can be defensibly trusted within a period of time [105]. However, it is not necessary to include all of the six TAs which could require huge effort. Instead, only some of them are necessarily taken into consideration according to a specific trust goal and environmental factors. The TAs are quantitatively or qualitatively measured based on different types of information and methodologies, which have been intensively explored over time [102]. Each TA can be slightly interpreted and attained differently depending on particular use-cases due to the variations and ambiguity of its linguistic meaning. Details of dependability models can be found on a large number of articles such as Cyber-Physical System (CPS) Framework [106] and Managing Information Security Risk [98] by the National Institute of Standards and Technologies (NIST).

TABLE 5-1. CHARACTERISTICS OF THE SYSTEM DEPENDABILITY IN DETAIL

	Attributes	**Meaning**	**Information**	**Target Entities**
System Dependability sub-TI	Confidentiality	Security and Privacy factor, measuring likelihood of the disclosure of sensitive information to unauthorized entities. Confidentiality could appear in Quality of Service and Quality of Information,	Authentication mechanisms, secret keys, security credentials, access control, privacy mechanism, encryption and decryption methods, anti-eavesdropping …	Network protocols, users
	Integrity	Security factor, measuring how well data/information is integrated.	Integrity suites including authorization scheme, correctness scheme, timeliness scheme or completeness mechanism	Network protocols, Network Devices

	Availability	Security factor, Ensuring timely and reliable access to and use of service. Certainty, accuracy, etc.	Service uptime, failure rate, intrusion resilience, hardware robustness, software robustness	Network protocols, Network Devices
	Serviceability/ Accountability	Accountability adds redundancy and responsibility of certain actions, duties and planning of the implementation of network security policies. Accountability itself cannot stop attacks but is helpful in ensuring the other security techniques are working properly.	Backup mechanisms, redundancy mechanisms, tolerance rate	Network systems
	Reliability	Need to understand the type and amount of uncertainty of the service. Certainty, accuracy, etc.	Consistency rate, timeliness, delay, jitter, anti-jamming mechanism	Network system
	Safety	A property to guarantee that an entity will not fail in a manner that would cause a great amount damage in a period of time.	Physical Risks and Cyber Risks should be considered	Network System, Network Device

Regarding to the IoT environment, we characterize two major TAs constituting the Benevolence dimension for Knowledge TI as Cooperativeness and Community-Interest illustrated as B1 and B2; and two TAs constituting the Integrity dimension as Honesty and Similarity, illustrated as I1 and I2, respectively.

- **Cooperativeness**: this property indicates the level of cooperativeness between a trustor and a trustee based on the following hypothesis: "the more cooperation between the two entities in a social network, the more trustworthy they are". Cooperativeness can be calculated by considering the common features between the two entities such as mutual friends and same locations.
- **Community-Interest**: Due to the integration of social networks in the IoT, the concept of community (of IoT entities) is also introduced that refers to a group of entities sharing the same characteristics (e.g., physical areas, the same goal, and same required tasks). This property indicates the level of community relationship between two entities based on the following hypothesis: "the more similarity among communities that entities belong to, the more trustworthy they get".
- **Honesty**: a property indicates the level of honesty of an entity based on observation toward an entity, of whether it conducts some suspicious interactions or it breaks social etiquette using a set of anomaly detection rules.
- **Similarity**: a property indicates the level of similarity between two entities (in terms of their features) using similarity measurement mechanisms between two profiles of entities [107]. This TA is taken into account because of the following hypothesis: "a trustor tends to trust a trustee if they are similar".

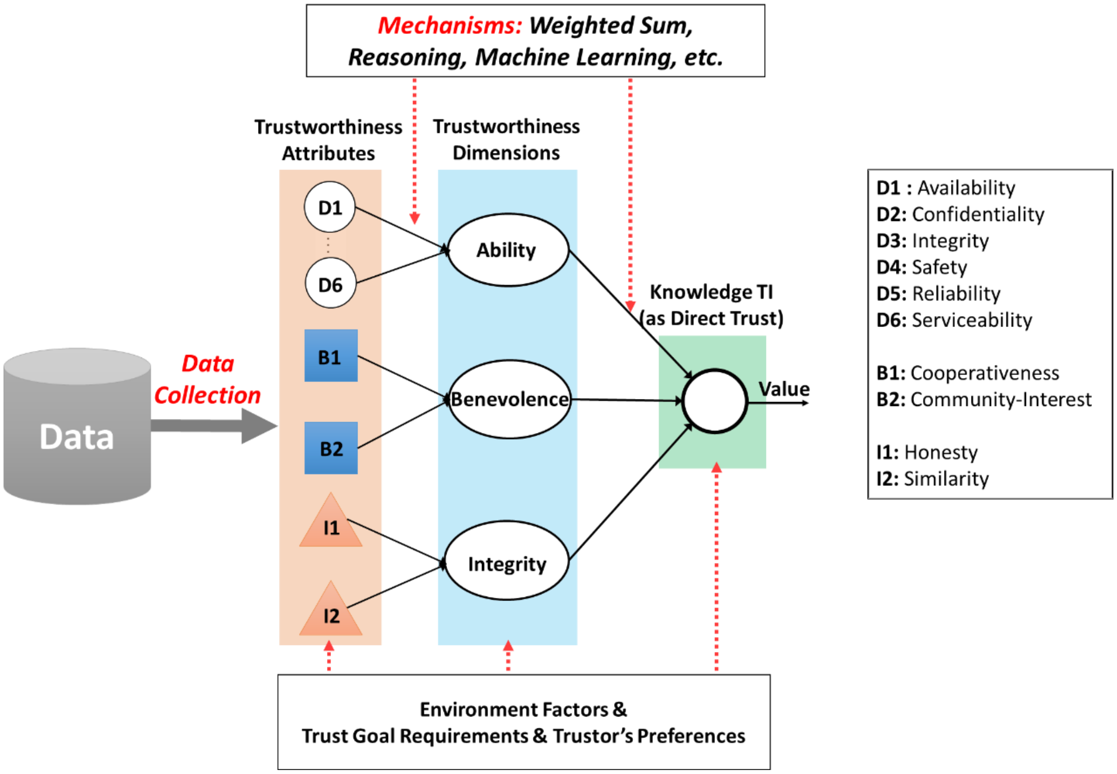


Figure 5-1. Evaluation model for direct trust (as Knowledge TI).

These four factors are chosen to determine whether an entity in a society is trustworthy or malicious; and also to recognize the IoT environment risks including various types of attacks in social networks such as self-promoting, bad mouthing, and ballot stuffing [101]. Therefore, the combination of these four TAs guarantees to explicitly indicate whether an entity is trustworthy in a social network or not. By integrating the Ability, a perceived trustworthiness in the IoT environment could be effectively achieved.

The existing models of these six concepts with corresponding attributes and measurement methodologies are characterized and converted into necessary information and knowledge; and then leveraged in a trust computation mechanism for calculating the related TAs and TIs. An importance of the trust computation is to manifest the trustor's preferences when combining attributes to obtain TAs and TIs. This can be done by weighting and/or policy-based methods in a trust reasoning mechanism. This process guarantees the subjective characteristic of trust.

5.2.2. Trust Attributes Extractions

- **Fuzzy Logic**

  To deal with wide range meaning of the Attributes in Knowledge TI which is ambiguous in some cases, the fuzzy-based approach is a prospective solution. Fuzzy Logic-based mechanisms provide ability to treat ambiguous data that is resolved only at runtime [108-110]; offering flexible, adaptive and extensive abilities for the system. Furthermore, fuzzy logic is able to represent vague terms like “low" or “high", “bad”, “acceptable” or “good”, which obviates the need to choose a specific value. With these advantages, fuzzy logic is widely used in control theory, pattern recognition and digital image processing.

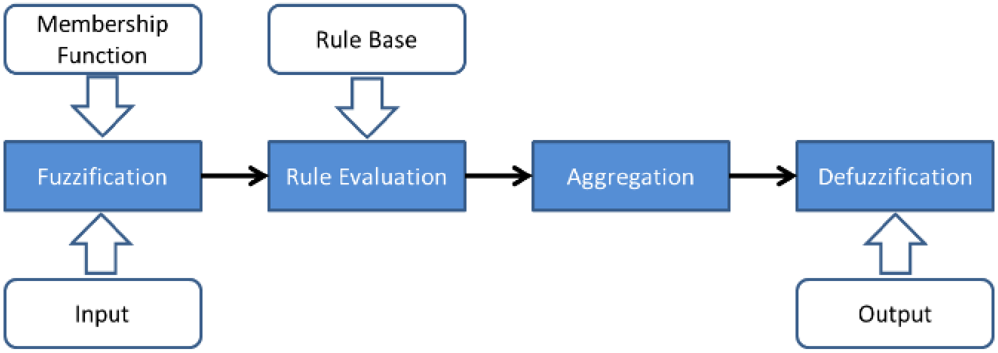


Figure 5-2. Mamdany Fuzzy Interference System procedures

For this purpose, the fuzzy approach is used for the Human-to-Vehicle Knowledge calculation. The ambiguous TAs parameters are easily represented (both by range of values or linguistic values where vagueness is associated). There are two well-known types of Fuzzy Information Systems (FIS): Mamdani FIS [111] and Sugeno FIS [112]. Mamdani FIS is used in our research work due to its greater expressive power and interpretability compared to Sugeno FIS [113].

The Mamdani FIS mechanism consists of four processes: Fuzzification, Rule Evaluation, Aggregation and Defuzzification as illustrated in Figure 5-2. To implement the fuzzy-based mechanism, several important factors such as input metrics, membership functions, and fuzzy rules are defined in accordance with service requirements that are registered to the trust platform. In Fuzzification step, the input for FIS is put as a real value, and then evaluated by applying appropriate membership functions.

- **Semantic Reasoning and Inference Engine**

  As the use of ontology brings many advantages in modelling the knowledge domain, we develop an upper ontology for modelling the Knowledge in the REK trust model. The ontology describes all generic concepts of trust and semantics among the concepts. It is a multi-level domain which covers all aspects of trust, from direct observation to third-party information, from physical to social layers of the network. Since it is an upper ontology, these concepts are the same across all trust scenarios (Figure 5-3). Note that different colours in the ontology concept showing the types class. If a class is primitive then its colour is yellow, otherwise if a class is already defined (with attributes and relationships), and then the colour is orange.

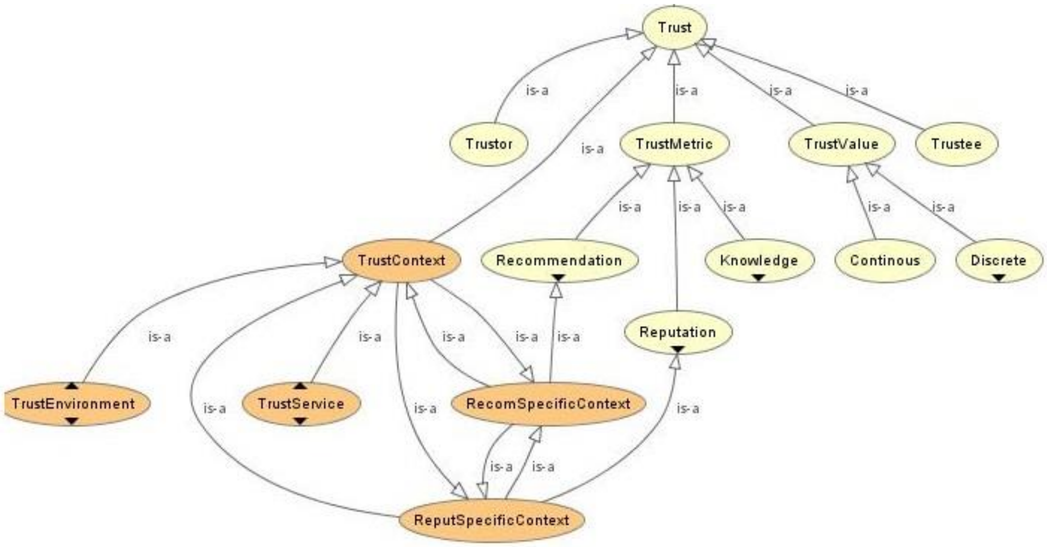


Figure 5-3. Trust Upper Ontology modelling RRK Trust Model

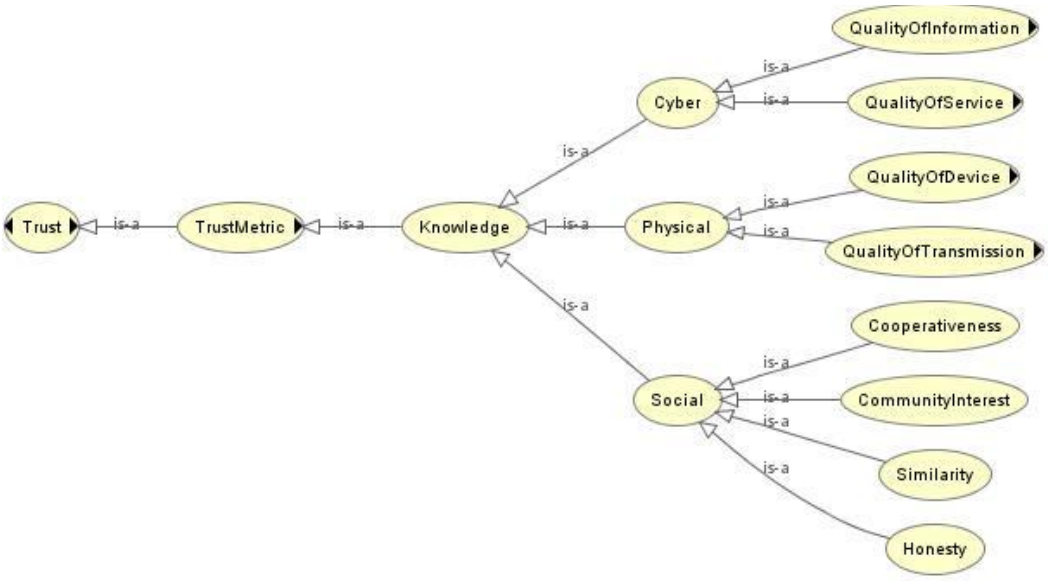


Figure 5-4. Knowledge TI in Trust Upper Ontology

The Knowledge TIs are derived from three sub-TIs called physical, cyber, and social. The reason is that each Knowledge sub-TI reflects different aspects of direct trust extracted from three layers of the IoT environment and CPSS systems. Each of them is comprised of TAs with different computational methods. For example, Social sub-TI is comprised of four TAs namely Honesty, Cooperativeness. Community-Interest and Similarity calculated based on social relationships using a mathematical model. Cyber sub-TI is constituted of Quality of Service and Quality of Information as illustrated in Figure 5-4. Each of them is calculated using an inference engine based on facts and rules derived from characteristics of cyber space. An example of Semantic Reasoning for the Knowledge TI in the Cloud web-hosting service use-case can be found in APPENDIX A: 1.

5.2.3. Trust Attributes Aggregation and Implementation Mechanisms

The conceptual trust computation procedures are illustrated in Figure 5-5 which is based on the previous concept illustrated in Figure 2-1. Trust is reached from the lowest step Awareness to the highest step Action when trust is obtained. To calculate trustworthiness, sufficient data about trustors, trustees and trust context needs to be collected, aggregated, processed and annotated in order to create semantic information which is a part of a trust knowledge base. The remainder of the trust knowledge base is in the form of rules acquired from the knowledge acquisition mechanism. The knowledge base is an input of an inference engine to infer new knowledge and then to reason a trust value. Base on the trust value, a decision could be made accordingly. Such important steps from Data Annotation and Collection to Decision Making are characterized as following:

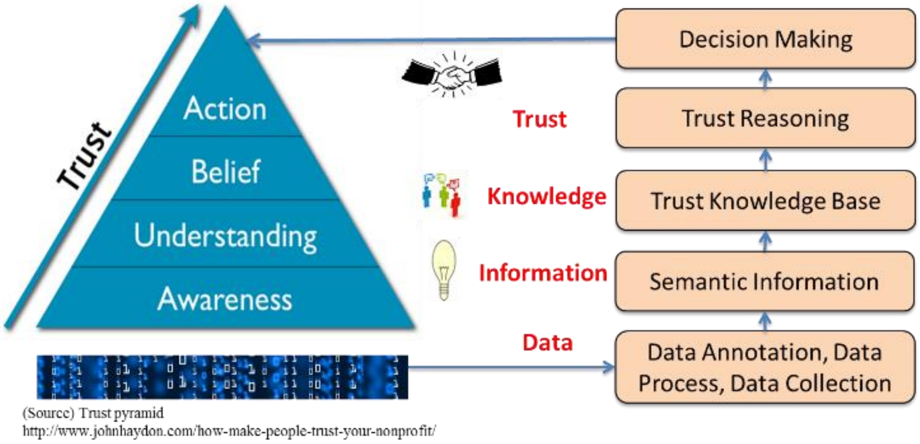


Figure 5-5. Conceptual Trust Evaluation Processes

- **From Data to Semantic Information**

  Trust-related data is collected from many kinds of sources in IoT. Various types of real-world observation data such as temperature, illumination, humidity, time, location, sound, and videos are from physical objects such as sensors and devices. Data is also from networking components such as uptime, bandwidth, packet delivery rate of a networking device; data encryption method and authentication mechanism of a data server. Data could also be from social space such as web-resident knowledge, information exchanged over social media, and relationships among entities in the IoT [2].

  Data is from heterogeneous data resources with different data characteristics and contains a large amount of information but only trust-related content is of interest. This leads to the need for a data integration and annotation framework along with an appropriate data model for data representation which is machinereadable and machine-interpretable. The framework is also required for enhancing semantic interoperability for producing semantic information.

In this study, several semantic web technologies are used for trust domain modelling, data integration, and data query. For more details, a trust domain is modelled using ontology in which trust-related data is annotated accordingly by using RDF schema. By doing so, raw data is transformed into semantic information as metadata in the form of RDF schema; and only information of interest is captured in accordance with the trust ontology. The data can be published using Linked Data so that it can be interlinked and enabled to semantic queries [114]. Several semantic web technologies such as SPARQL[115], an SQL-like language, can be used to query the RDF triple store.

- **From Semantic Information to Trust Knowledge Base**

  Trust knowledge base can be fundamentally understood as trust-related structured and unstructured information represented in a machine-interpretable language (knowledge representation), such as First Order Logic, in order for reasoning trustworthiness by using an inference engine. The creation of the trust knowledge base includes the creation of facts about trust (declarative knowledge) and the creation of logics among concepts contained in the facts (procedural knowledge) [116]. We tend to use a combined knowledge representation formalism which integrates both rule-based language and ontology for supplying advanced reasoning capabilities.

  Trust-related data is captured and annotated using the ontology with RFDS for producing semantic information. This semantic information is considered as facts in the trust knowledge base, as it is represented in the ontology language in the form of DLs [117]. The rules can be represented in the form of both monotonic rules and non-monotonic rules to express knowledge about concepts from the ontologies such as classes, sub-classes, instances and relations. The rules are the most important part of the trust knowledge base that interprets meaning and describes relationships of the concepts included in the facts. Based on the set of rules, the inference engine can draw new knowledge, new facts that we are interested in. Generally, rules are typically in IF-THEN form:

```
IF A1, A2,…, Am THEN B1, B2,…, Bn
ELSE C1, C2, ..., Ct
```

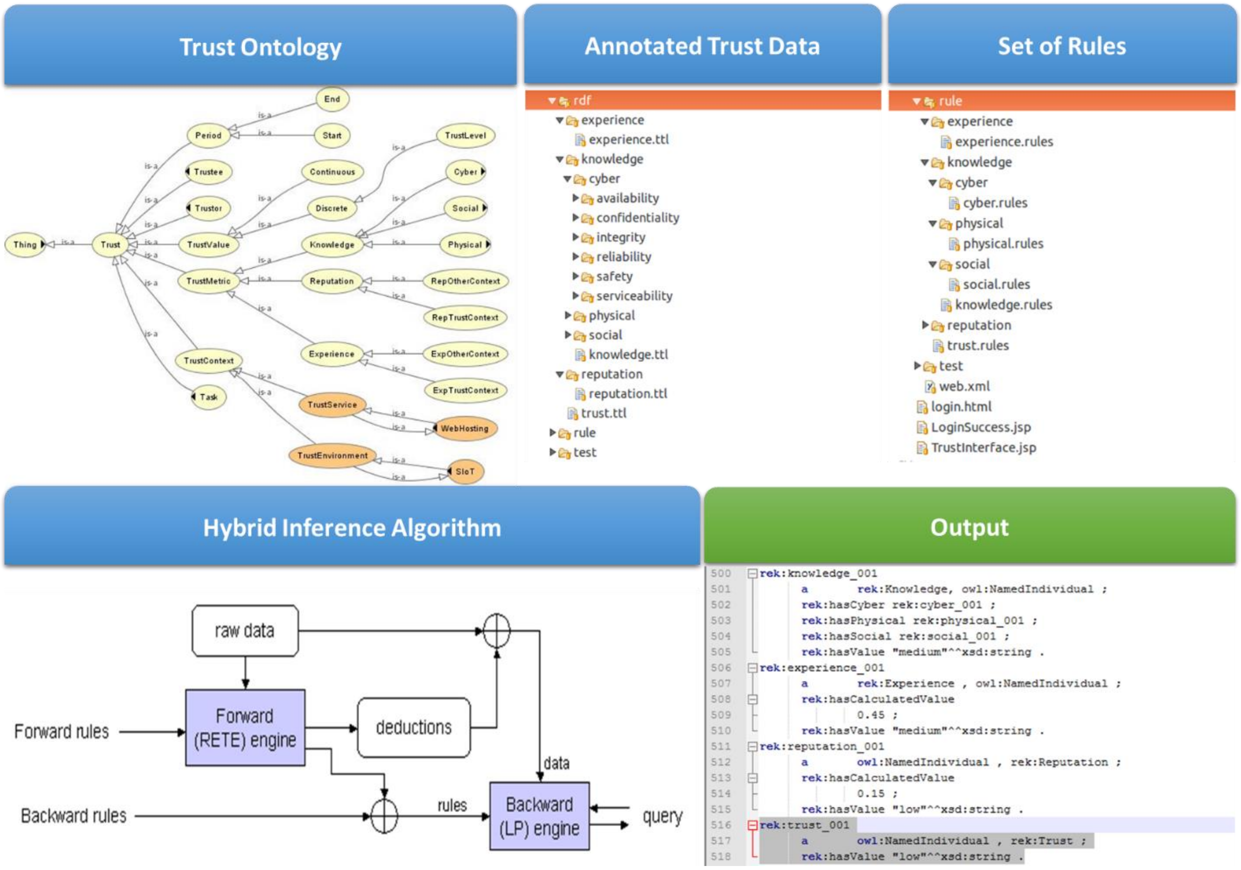
whereas Ax | x = (1,m); By | y=(1,n); and Cz | z=(1,t) are logical expressions. Commas denote conjunction on all sides. The word THEN is to draw conclusions, implies several meanings, depending on the type of logic used in knowledge representation. Depending on each rule engine and reasoner used for reasoning trustworthiness, rules are encoded in different syntaxes such as Jena and Pellet.

The process to create rules for a knowledge base is called knowledge acquisition, a part of knowledge engineering [118]. Technically, knowledge acquisition is a complicated process that acquires knowledge, here it is in terms of rules, from many resources such as human experts, data, documents, Internet resources, etc., using many methods such as interviews with human experts; and applies data mining and machine learning mechanisms with data and Internet resources.

- **Trust Reasoning Mechanism**
  A semantic reasoner is used for inferring new knowledge related to trust including facts about TAs, TIs and trust values. The final goal is to compute trustworthiness based on the trust knowledge base. In this study, the trustworthiness is simply defined in three levels: low, medium and high meaning distrust, normal and trust, respectively. The reasoner takes the trust knowledge base as its input and infers new knowledge as new facts, as a result, additional rules in the knowledge base are triggered; new other facts could be created. This process would iterate until a goal has been reached or no rules can be matched.

  There are two approaches for inferring new knowledge called forward chaining and backward chaining. Forward chaining approach starts with known facts and infers new facts by cycling the reasoning process until there are no additional rules that can be triggered meaning that all new facts are already asserted. By looking at the new facts after the reasoning process has been done, a goal could be obtained. Conversely, backward chaining reasoning approach starts with a goal and traces backward by determining what facts must be asserted and what rules need to be used in order to obtain that goal. This process is iterated and if all facts and rules used for inferring the goal are included in the knowledge base, this means that the goal has been achieved, otherwise, the goal cannot be inferred by that knowledge base.

  Since Apache Jena framework is used in the use case demonstration, there are various types of integrated inference engines including the generic rule-based reasoner that enables user predefined rules. The Jena integrated rule-based reasoner supports both forward chaining, tabled backward chaining reasoning strategies as well as the hybrid approach. For example, generic reasoner supported in Jena with forward chaining mode is used in the demonstration to infer new facts and look for the facts, here are the trust levels, which we are interested in.



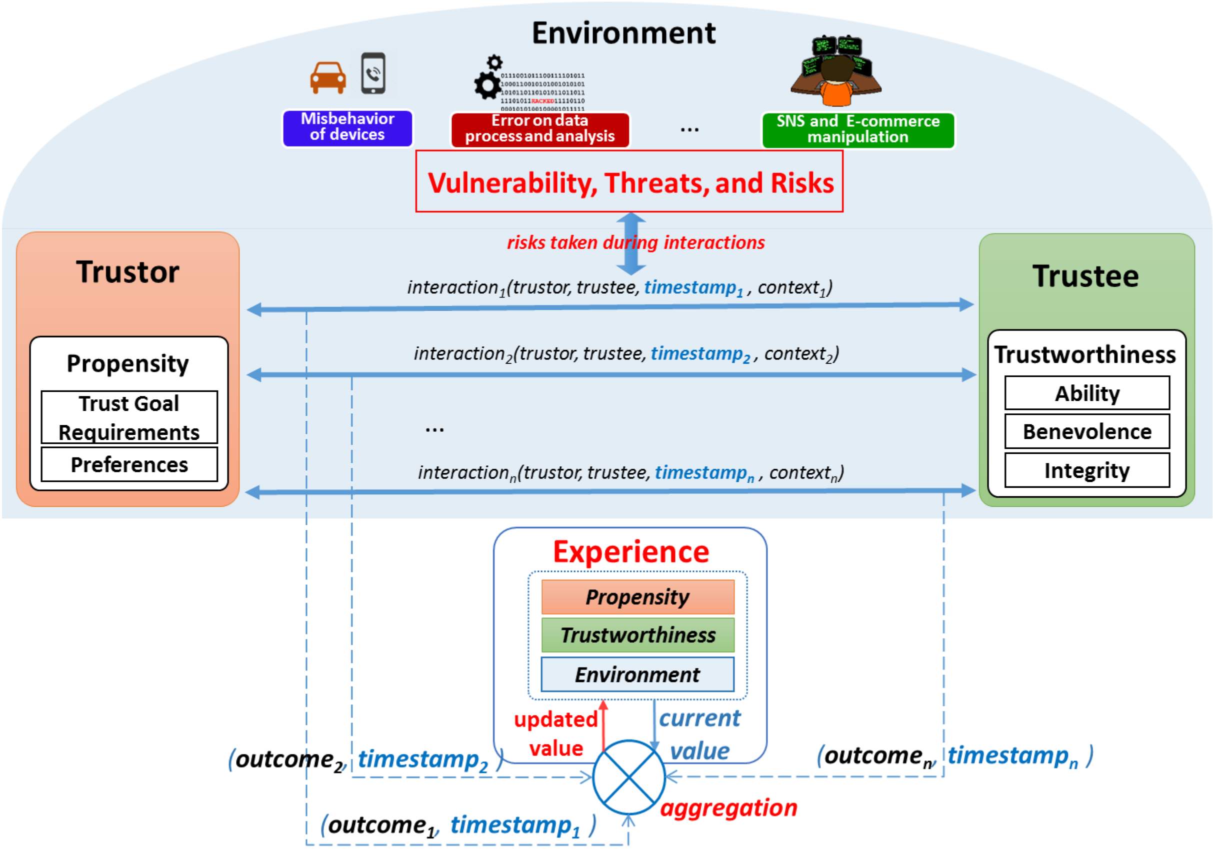
```
rek:knowledge_001
        a       rek:Knowledge, owl:NamedIndividual ;
        rek:hasCyber rek:cyber_001 ;
        rek:hasPhysical rek:physical_001 ;
        rek:hasSocial rek:social_001 ;
        rek:hasValue "medium"^^xsd:string .
rek:experience_001
        a       rek:Experience , owl:NamedIndividual ;
        rek:hasCalculatedValue
                0.45 ;
        rek:hasValue "medium"^^xsd:string .
rek:reputation_001
        a       owl:NamedIndividual , rek:Reputation ;
        rek:hasCalculatedValue
                0.15 ;
        rek:hasValue "low"^^xsd:string .
rek:trust_001
        a       owl:NamedIndividual , rek:Trust ;
        rek:hasValue "low"^^xsd:string .
```

Figure 5-6. A demonstration of Trust Aggregation Framework leveraging Semantic Web Technologies

For example, a generic reasoner with hybrid-mode is used to infer level of trust as the final goal as shown in the Hybrid Inference Algorithm and Output parts in Figure 5-6. As can be seen in the figure, the facts are written in t he ttl format files: experience.ttl, reputation.ttl and knowledge.ttl. The set of rules for the reasoning mechanisms are written in some files: experience.rules, cyber.rules, physical.rules, etc. The final goal is to infer the trust value for the set of information from facts and rules. The trust value at the moment is "unknown". Using the Inference engine over the facts and rules, the output can be infered as trust_001: low, meaning that the final trust value inferred from the facts (i.e., knowledge_001, experience_001, reputation_001 instances) and rules is "low", which is the value we are looking for.

5.3 Experience Trust Indicator

We propose a conceptual model for the Experience TI depicted in Figure 5-7 which computes experiences based on the three factors: the current value of Experience, the outcomes, and the timestamps of individual interactions. Therefore, an outcome evaluation scheme for the interactions is one of the important components in the Experience TI model. Various mechanisms can be used to deduce outcomes of interactions depending on particular scenarios. For instance, outcomes might be feedback (in both implicit and explicit forms) from consumers after each interaction (as used in many e-Commerce and reputation systems), or might just be a Boolean value (or 0/1) generated by using an ACK message to track whether the interaction has been successfully accomplished or not (as in some reputation-based trust systems). For example, in Wireless Sensor Networks, interactions are package transmissions between two nodes, if a transmission is successful, then the outcome of the interaction is 1, and 0 otherwise. In file-sharing P2P networks, interactions are file transfer transactions. If a file is successfully transferred, then the outcome of the interaction is 1; otherwise it is 0. The interaction is also in the form of any type of relationship between two entities. For example, Google PageRank considers a hyperlink as an interaction between a source webpage and a destination webpage; and the outcome value is set as 1 [42].



Environment
Misbehavior of devices
Error on data process and analysis
...
SNS and E-commerce manipulation
Vulnerability, Threats, and Risks
risks taken during interactions
Trustor
Propensity
Trust Goal Requirements
Preferences
interaction$_1$(trustor, trustee, timestamp$_1$, context$_1$)
interaction$_2$(trustor, trustee, timestamp$_2$, context$_2$)
...
interaction$_n$(trustor, trustee, timestamp$_n$, context$_n$)
Trustee
Trustworthiness
Ability
Benevolence
Integrity
Experience
Propensity
Trustworthiness
Environment
updated value
current value
aggregation
(outcome$_2$, timestamp$_2$)
(outcome$_1$, timestamp$_1$)
(outcome$_n$, timestamp$_n$)

Figure 5-7. The experience TI model in the REK trust evaluation.

5.3.1. Mathematical Model and Analysis

Another important component is an aggregation model for calculating Experience TI. There is an important assumption about the experience relationship between humans in the sociological environment: experience accumulates for cooperative interactions and is decreased by uncooperative interactions. It also tends to decay over time if it is not maintained by interactions. This assumption has been reasonably proven in much of the trust-related sociological literature [119, 120]. Thus, there are three trends of the experience relationship: Increase, Decrease, and Decay; and all of them are measured based on three features: intensity of interactions, values of the interactions, as well as the current value of the experience. Therefore, a mathematical linear difference equation could be used to model the trends of the Experience TI. We have proposed an Experience TI model in which an outcome of an interaction is either 0 (indicates uncooperative interaction) or 1 (indicates the cooperative interaction). The model consisting of three trends is proposed as following:

- **Increase (due to cooperative interactions)**

  Let ϑ is the interaction score, normalized in the range [0, 1]. A cooperative interaction is when $\vartheta > \theta_{co}$ threshold. The increase is modelled using a linear difference equation as follows:

$$Exp_{t+1} = Exp_t + \vartheta_t \times \Delta Exp_{t+1} \tag{5-1}$$

$$\Delta Exp_{t+1} = \alpha \times (1 - \frac{Exp_t}{max_{Exp}}) \tag{5-2}$$

  where Exp_t is the Experience value at the time t. initExp is the initial value of the Experience. α is the maximum increase value, and max_{Exp} is the maximum Experience value ($\alpha < max_{Exp}$).

  Experience accumulates from cooperative interactions and accumulated values depending on both QoD score ϑ_t and the current value Exp_t. With this increase model, Experience forms a curve that is incremental and asymptotic to 1. More and more cooperative interactions are required to get a higher value, indicating that strong relationships are difficult to achieve.

- **Decrease (due to uncooperative interactions)**

  An uncooperative interaction is when the QoD score $\vartheta < \theta_{unco}$ threshold. The Decrease model is as follows:

$$Exp_{t+1} = Max\langle min_{Exp}, Exp_t - (1 - \vartheta_t) \times \beta \times \Delta Exp_{t+1}\rangle \tag{5-3}$$

  where ΔExp_{t+1} is determined by Equation (2); β is rate of decrease parameter that is normally greater than 1 because Experience is difficult to gain but easy to lose. min_{Exp} is the minimum Experience value. According to Equation (3), it is easy to see that strong relationships are more resistant to uncooperative interactions whereas weak relationships are severely damaged.

- **Decay (due to no interactions or neutral interactions)**

  In sociology, relationships between people decay over time if participants do not interact, although the decay rates are different depending on the strength of the relationships [121]. Similarly, Experience decays if there is no transaction after a period of time or interactions are neutral (i.e., $\theta_{unco} < \vartheta < \theta_{co}$). Decay value is assumed to be inversely proportional to current Experience value, thus strong relationships exhibit less decay than the weak ones. If the current status is high (meaning that there is a strong tie between two entities) then the decrease is not much; but if current status is low (i.e., a weak tie between the two) then the decrease is much. Hence, experience is assumed to require periodic maintenance but strong ties tend to persist longer even without reinforcing cooperative interactions. Then, the mathematical model for the Experience Decay is proposed as following:

$$Exp_{t+1} = Max\langle init_{Exp}, Exp_t - \Delta decay_{t+1}\rangle \tag{5-4}$$

$$\Delta decay_{t+1} = \delta \times \left(1 + \gamma - \frac{Exp_{t-1}}{max_{Exp}}\right) \tag{5-5}$$

where δ is the minimal decay value which guarantees that even strong relationships still get decreased; and γ is the decay rate. Similar to the Decrease model, strong Experience relationships decay much more slowly than weak ones. Relationships require periodic maintenance, but strong ones tend to persist longer even without reinforcing cooperative interactions.

According to the Experience TI model, in order to obtain a high experience value (i.e., a strong tie between a trustor and a trustee), it is required to have many cooperative interactions in a short duration of time. And when it gets high, it is not easy to decay as time goes by. However, uncooperative interactions can highly damage the experience relationship, especially when the current state is not strong. This is similar to what happens in the real human world, thus, we believe the proposed Experience TI model can effectively migrate the experience relationship from the human sociology environment to entities in the IoT.

5.3.2. Implementation Mechanism

We simulate the proposed Experience TI model in Matlab. For convenience and consistency, Experience TI values are normalized to the range [0, 1] (i.e., $min_{Exp} = 0$ and $max_{Exp} = 1$). Consequently, equation (1) and (2) can be rewritten as either:

$$Exp_{t+1} = Exp_t + \alpha \times (1 - Exp_t) \tag{5-6}$$

$$Exp_{t+1} = (1 - \alpha) \times Exp_t + \alpha \tag{5-7}$$

The source code for the simulation can be found here[3]. Parameters settings in the simulation are explained in Table 5-2.

TABLE 5-2. PARAMETERS SETTINGS FOR THE SIMULATION OF EXPERIENCE TI

[3] https://github.com/nguyentb/Experience_Reputation_Trust/blob/master/Experience_model.m

Parameters	Values	Parameters	Values
max_{Exp}	1	γ	0.005
min_{Exp}	0	δ	0.005
$init_{Exp}$	0.3	$\theta_{uncooperative}$	0.3
α	0.1	$\theta_{cooperative}$	0.6
β	2		

As shown in the equation (5-2) and (5-6), the increase value $\Delta Exp_{t+1} = \alpha \times (1 - Exp_t)$ is relatively large when the current value Exp_t is small and vice versa. The mathematical solution of such linear difference equation (7) is simple that Experience TI will reach to 1 in a log scale. This is also proven using the simulation illustrated in Figure 5-8 that the Experience TI development curve is an asymptote to 1. The loss model and decay model also form log curves which make the Experience TI less susceptible if a relationship is strong tie and vice versa.

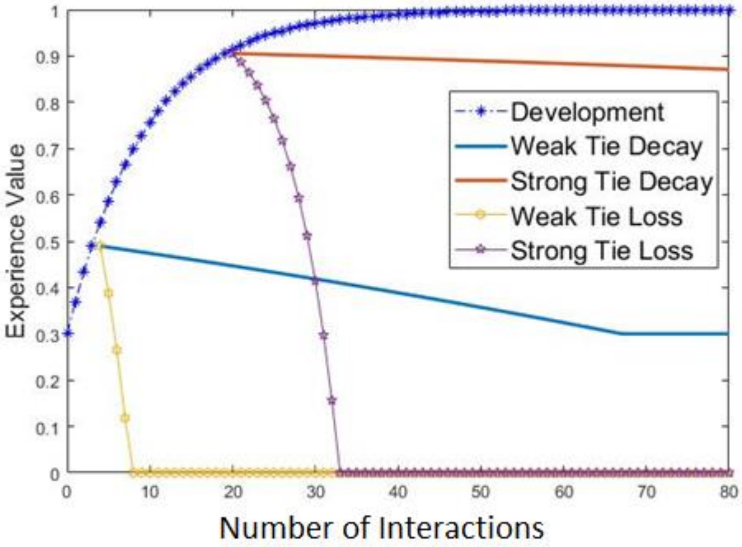


Figure 5-8. Experience Model with Development, Loss and Decay trends

Therefore, in order to achieve high Experience TI (strong tie between two entities), it is required to have many cooperative interactions consecutively; and when it gets high, it is not easy to decay as time goes by. As can be seen in Figure 5-8, decay values depend on the current status of a relationship: a strong tie decays much more slowly than a weak tie. Hence, the relationship is assumed to require periodic maintenance but strong ties tend to persist longer even without reinforcing cooperative interactions.

However, uncooperative interactions can highly damage the relationship even with strong ties. The loss rate $\beta = 2$ means that Experience TI loses twice (due to an uncooperative interaction) compared to what it has gained (due to a cooperative interaction) as demonstrated in Figure 5-8. This is similar to what happens in the real human world, thus, we believe the proposed Experience TI model can effectively migrate the experience relationship from the human sociology environment to entities in the IoT.

5.4 Reputation Trust Indicator

According to the Experience TI model, some entities which have interacted with the trustee hold their opinions about the trustee as their experiences. Therefore, if these entities share their opinions about the trustee's trustworthiness (the shared opinions are as recommendations on the trustee), an aggregation model can be leveraged to combine these recommendations to a unique value as Reputation. In the IoT environment with billions of entities, only a small number of entities have interacted with one another, and there is a very high possibility that two any entities in the IoT are new to each other, thus, there is no Experience between the two. Therefore, Reputation TI is a crucial indicator for trust, especially in the case where there are no previous interactions between a trustor and a trustee; and a reputation system should also develop an incentive scheme to encourage entities to share their experiences, resulting in better reputation results.

5.4.1. Mathematical Model

A necessary consideration when designing a reputation model is that each recommendation differently contributes to the reputation of an entity as illustrated in Figure 5-9. The weight of a recommendation from entity x to entity y depends on both experience value $Exp(X,Y)$ as well as Reputation value of the entity X itself $Rep(X)$. It is understandable because, besides experience values, recommendations from high reputation entities are more valuable than from the lower one's. Moreover, a recommendation could be supportive or unsupportive specified by a threshold parameter θ. That is, if $Exp(i,X) \geq \theta$ the recommendation from entity i to entity X is supportive, resulting in increasing X*'s* reputation whereas if $Exp(j,X) < \theta$ the recommendation is unsupportive, resulting in reputation decrease. Based on these two observations, and inspired by Google PageRank idea, we have proposed a novel mathematical model for Reputation TI as follows:

As an overall opinion, the calculation of Reputation of a user U, denoted as $Rep(U)$, requires taking all users that have prior experience with U into consideration. Thus, Reputation can be quantified using a graph analysis algorithm on the Experience relationship topology, which is somewhat similar to the Google PageRank [42] and the weighted PageRank [126]. The difference from the two previous models is that each user i contributes differently to $Rep(U)$, in either a positive or negative manner, depending on both $Exp(i,U)$ (i.e., the Experience from i toward U) and the user's Reputation (i.e., $Rep(i)$). The PageRank models proposed in [42] [126] are modified by dividing the Experience topology into two sub-groups: Positive Experiences (i.e., $Exp > \theta$) and Negative Experiences (i.e., $Exp < \theta$) where θ is a predefined threshold. Then, the Reputation model is proposed as follows:

- **Positive Reputation**

$$Rep_{Pos}(U) = \frac{1-d}{N} + d \times \left(\sum_{\forall i} Rep_{Pos}(i) \times \frac{Exp(i,U)}{C_{Pos}(i)} \right) \tag{5-8}$$

where: $C_{Pos}(i)$ = $\sum_{Exp(i,j)>\theta} Exp(i,j)$ is the sum of all positive Experience from the user i.

- **Negative Reputation**

$$Rep_{Neg}(U) = \frac{1-d}{N} + d \times \left(\sum_{\forall i} Rep_{Neg}(i) \times \frac{1-Exp(i,U)}{C_{Neg}(i)} \right) \tag{5-9}$$

where: $C_{Neg}(i) = \sum_{Exp(i,j)<\theta}(1- \; Exp(i,j))$ is the sum of all compliment of negative Experience from the user i.

- **Overall Reputation**

$$Rep(A) = \max\left(0, Rep_{Pos}(U) - \; Rep_{Neg}(U)\right) \tag{5-10}$$

Where:

$Rep(i)$ is the reputation of the entity i that we are interested. Equation (10) guarantees that Reputation TI values are not below min_{Rep} (i.e., 0).

N is total numbers of entities in the networks for calculating Reputation

d is the damping factor. Various studies on web ranking have tested different damping factors and come up at 0.85.

$Exp(i,X)$ is Experience TI from the entity i toward the entity X described in Section III.

$Rep_{Pos}(i)$is positive reputation of the entity i which considers only supportive recommendations.

$C_{Pos}(i)$= $\sum_{Exp(i,j)>\theta} Exp(i,j)$is the total values of all experiences in supportive recommendations that the entity i is currently sharing.

$Rep_{Neg}(i)$ is negative reputation of the entity i which considers only unsupportive recommendations.

$C_{Neg}(i) = \sum_{Exp(i,j)<\theta}(1- \; Exp(i,j))$ is total compliments of experiences in all negative recommendations that the entity i is currently sharing.

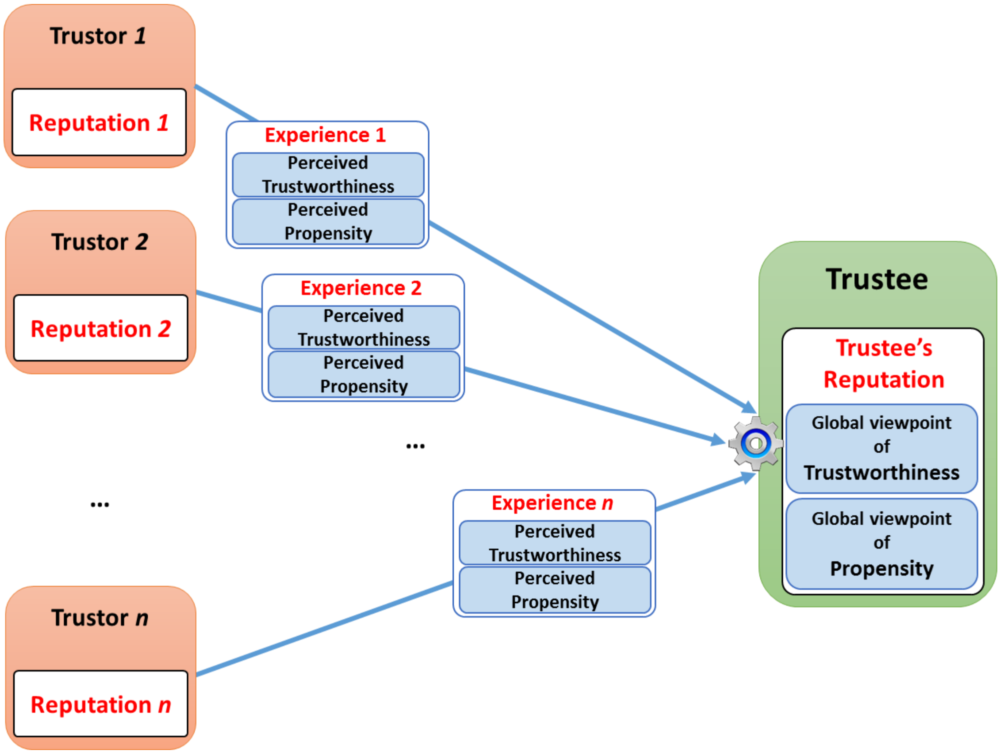


Figure 5-9. Weighted PageRank-based Reputation Model incorporating the Experience concept

5.4.2. Analysis and Discussion

According to the equation (5-8), let M is the $N \times N$ diagonal matrix where the diagonal element $m_i = C_{Pos}(i);\ \forall i = \overline{1,N}$. Let Exp_{Pos} is a $N \times N$ matrix that:

$$Exp_{Pos}(i,j) = \begin{cases} Exp(i,j) \text{ if } Exp(j,i) \geq \theta \\ 0 \text{ otherwise } (Exp(j,i) < \theta) \end{cases} \qquad (5\text{-}11)$$

And let Rep_{Pos} is the vector of the positive reputation $Rep_{Pos}(i)\ \forall i = \overline{1,N}$. Then, recall Equation (5-8) we come up with the formula in matrix notation:

$$Rep_{Pos} = \left(\frac{(1-d)}{N} E + \mathrm{d} \times Exp_{Pos} \times M^{-1}\right) \times Rep_{Pos} \qquad (5\text{-}12)$$

where E is $N \times N$ matrix of 1s. Let $A = \left(\frac{(1-d)}{N} \times E + \mathrm{d} \times Exp_{Pos} \times M^{-1}\right)$, then Equation (5-12) is rewritten as:

$$Rep_{Pos} = A \times Rep_{Pos} \qquad (5\text{-}13)$$

Thus, $Rep_{Pos}$is an *eigenvector* of matrix A with *eigenvalue* = 1.

We now should prove that Rep_{Pos} exists and is unique (i.e., it is not ambiguously defined), resulting in that the positive reputation of any entity $Rep_{Pos}(X)$ is successfully determined. Equations (5-12) and (5-13) are reminiscent of the stationary distribution of a Markov chain of random process that moves among the set of states numbered *1* to N with an $N \times N$ transition matrix P where P(*go from state i to state j*) = P(*i,j*). Thus, consider a Markov chain in which the states are as the N entities with the transition matrix P as the transpose matrix of A, thus:

$$P(i,j) = A^T(i,j) = A(j,i) = \frac{(1-d)}{N} + \mathrm{d} \times \frac{Exp_{Pos}(j,i)}{m(j)} \tag{5-14}$$

Consequently, the Markov chain can be defined as follows:

$$P(i,j) = \begin{cases} \frac{(1-d)}{N} + \mathrm{d} \times \frac{Exp_{Pos}(j,i)}{m(j)} \text{ if } Exp(j,i) \geq \theta \\ \frac{(1-d)}{N} \text{ otherwise } (Exp(j,i) < \theta) \end{cases} \tag{5-15}$$

Fortunately, this turns to a *random suffer* model with *random jumps*. This leads to the Markov chain being strongly connected, and the Rep_{Pos}vector, which is the stationary distribution of the Markov chain, being unique[42], [126], [127],[128]. Similarly, the Rep_{Neg}vector from Equation (5-9) exists and is unique. Therefore, the Reputation TI defined in Equation (5-10) also exists and is unique.

5.4.3. Simulation and Results

The Reputation TI for all entities in a network can be calculated using Equations (5-8), (5-9) and (5-10) either algebraically or iteratively. Using the algebra traditional method to solve the matrix equations (5-8) and (5-9) takes roughly N^3 operations which is a big concern when the size of a network dramatically increases. We, therefore, use the iterative method which is much faster [129]. Therefore, there is a need to validate the correctness (convergence) of the proposed Reputation mechanism, as well as the effectiveness of the mechanisms (number of interaction to reach to accurate results). Equations (5-8), (5-9), and (5-10) form a normalized probability distribution after conducting a number of iterations throughout the network; reputation values for all entities in the network are updated after each iteration. For a clear visualization of the algorithm convergence, we do not normalize the reputation values to the range [0, 1], instead the reputation values will be in the range of the network size.

Regarding to the simulation of the convergence and effectiveness of the proposed Reputation mechanism, we have implemented the simulation in Matlab that can be found here[4]. Figure 5-10 depicts the convergence rate for the network size N=100, 400 and 800 with the tolerance = 10^{-3} which is accurate enough for ranking

[4] https://github.com/nguyentb/Experience_Reputation_Trust/blob/master/Reputation_model.m

of entities in the range [0, N]. The tolerance is defined as the *2-norm* vector of the difference between Rep vectors in two consecutive iterations.

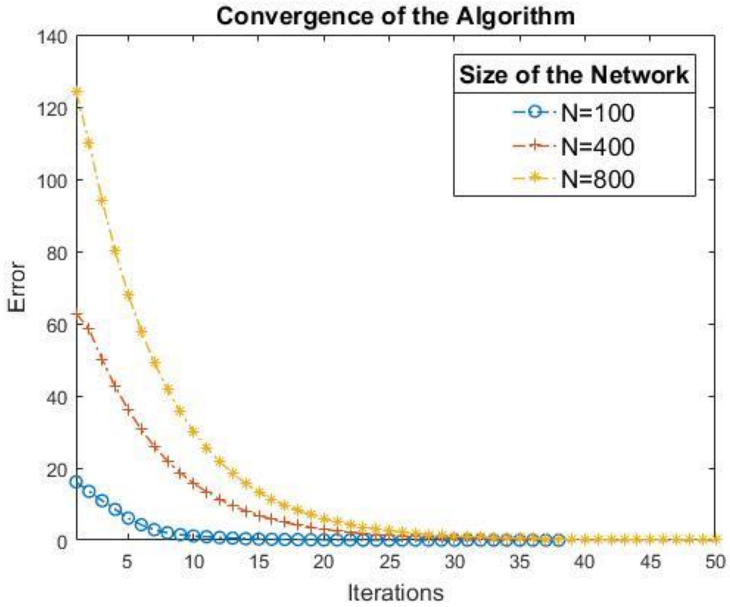


Figure 5-10. Convergence of the proposed Reputation TI algorithm with several network sizes

As can be seen from the graph in Figure 5-10, the Reputation TI model converges to a reasonable tolerance (i.e., 10^{-3}) in 50 iterations. The convergences on half and one eighth of the data take 42 and 38 iterations, respectively.

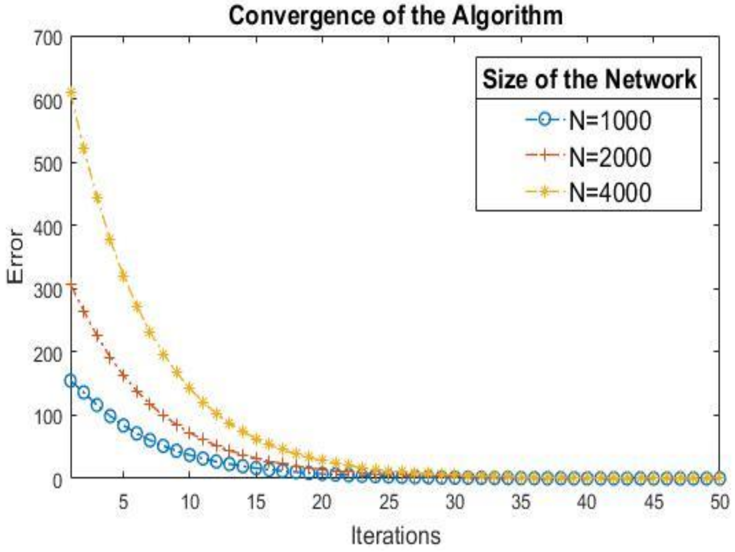


Figure 5-11. Convergence of the Reputation TI algorithm with real data from Wise-IoT project

Figure 5-11 depicts the convergence of the Reputation mechanism using the real data from users' feedback of the smart parking service developed and deployed in the Wise-IoT project. In this instance, we consider larger number of network size (i.e., 1000 to 4000 entities including users and sensor devices) and observe the same results. This graph suggests that this reputation model will scale well even for a large network size as the scaling factor is roughly linear in log n. Therefore, the reputation model can be implemented in a centralized system to calculate reputation values for all entities in a social network. Similar mechanisms for calculating rankings can be found in various related-literature [42, 126-128].

However, the implementation might be challenged when the size of a network is extremely high (i.e., the IoT network with billions of entities) due to memory size requirements for managing all experiences among entities. This could be solved by using classification algorithms with an appropriate semi-distributed architecture so that a network can be divided into smaller sub-populations, resulting in the feasibility of conducting the proposed reputation model.

5.5 Finalize Trust from Trust Indicators

The outcome of the REK Trust Evaluation model is aggregated based on the triad, Reputation, Experience, and Knowledge TIs. It also requires the aggregation of TAs to derive Knowledge TI. As clarified in the conceptual trust model as well as the REK model, these aggregations should take both environmental factors and trustor's propensity into consideration. There are a variety of techniques for combining the TAs and TIs such as Bayesian neural networks, fuzzy logic and machine learning depending on specific use-cases and individual users' preferences.

5.5.1. Weighted Sum

The first approach is to use mathematical models such as weighted sum [130, 131], Bayesian neural networks [132, 133], and machine learning algorithms such as linear regression [134]. These models use mathematical models to express a trustor's propensity and environment conditions by assigning weights for individual features (i.e., TAs and TIs). These values can be autonomously updated depending on outcomes of the models by using a feedback mechanism.

A trust value is an aggregation of the Knowledge, Experience and Reputation values. There are a variety of techniques for combining the two TIs such as Bayesian neural networks, fuzzy logic and machine learning depending on specific use-cases and individual users' preferences. For example, a simple weighted sum for calculating a final trust value between trustor A and trustee B is as follows:

$$Trust(A,B) = \alpha Knowledge(A) + \beta Exp(A,B) + \gamma Rep(B) \quad (5\text{-}16)$$

where $\alpha, \beta, \gamma > 0$ are weighting factors satisfying $\alpha + \beta + \gamma = 1$. The weighting factors can be autonomously tuned using other techniques such as machine learning and semantic reasoning.

5.5.2. Reasoning Mechanisms

The second method makes use of an inference engine for inferring new knowledge from a knowledge-base such as reasoning mechanisms [116] and fuzzy-based mechanisms [86, 135, 136]. These inferring mechanisms are frequently used for deriving causal-consequence knowledge that is also appropriate for incorporating a trustor's propensity and environmental factors. In the second approach, all trust-related information already obtained (e.g., TAs, Experience TI, and Reputation TI) are represented in the form of facts; trustor's propensity and environmental factors are represented in the form of logic applied upon the facts (e.g., rules in reasoning mechanisms, and membership functions in fuzzy-based mechanisms). Based on the set of logic, an inference engine can draw new knowledge that is of interest such as Knowledge TI and the overall trust value. In real implementation, a set of default logics should be already investigated and deployed for all entities. Then a trustor might have more preferences or a considered environment might have different conditions; then these factors are converted into logics that replace or supplement the default set of logics, which is already introduce in Section 5.2.3.

5.6 Chapter Summary

This article opens many research directions in order to fulfil the trust evaluation framework. One of the most important studies is to develop intelligent rule creation for the trust knowledge base. In this demonstration, rules are predefined using our understanding of specific services with user preferences on trust. This will be improved by using machine learning techniques for rule pattern recognition for an automatic rule creation mechanism. A verification mechanism is also needed to check the quality of the knowledge base for issues with consistency and redundancy. Another research direction could be the improvement of the reasoning mechanism so that it can autonomously adapt with the changes of the knowledge base, resulting in an autonomous trust computation framework and with data streaming (stream reasoning). The usage of Semantic Web technologies such as the Ontology, RDFS and reasoning mechanism could also be improved for more complex use cases and for the support of real-time processing and scalability. Finally, we consider some potential methods for combining those TAs of the Knowledge TI, the Experience TI and the Reputation TI such as weighted sum; reasoning and inference mechanisms for finalizing the overall trust value as the final goal of the REK trust evaluation mechanism.

CHAPTER 6. UTILIZE REK TRUST EVALUATION IN MOBILE CROWD-SENSING

6.1 Introduction

The emerging Internet of Things (IoT) applications and services heavily depend on data collected from sensing campaigns such as sensor networks and crowd-sourcing. Traditional sensor network schemes deploy sensors in the terrain to acquire a variety of aspects of human lives which have never reached full potential and been successfully implemented in the real world. This is due to some unsolvable challenges such as high installation cost and insufficient spatial coverage [137]. The new sensing paradigm called Mobile Crowd-Sensing (MCS), which is a sort of crowd-sourcing leveraging built-in sensors and applications in smart mobile devices, has recently been considered as a promising solution for IoT sensing campaigns [138]. MCS allows increasing numbers of mobile devices owners to share their own data acquired by sensors and social applications; in exchange, device owners get incentives for their contributions. Data collected from user devices are diverse such as local news, noise level, traffic conditions, and social knowledge. With diversified spatial coverage due to the mobility of large-scale mobile users, MCS is expected to enable a variety of IoT services including public safety, traffic planning, environment monitoring, and social recommendation. This human-powered sensing approach augments capabilities of existing IoT infrastructures without additional costs, resulting in a win-win strategy for both users and IoT systems.

However, MCS also imposes some critical challenges such as cross-space data mining, retaining privacy and providing high-quality data [139]. Low-quality data could lead to numerous difficulties in providing high-quality services or even damage MCS systems. Certain methods have been proposed for improving quality of data (QoD) in MCS including estimation and prediction of sensing data along with statistical processing for identifying and removing outliers in sensing values [17]. Data selection techniques are also used to filter low-quality or irrelevant data and to generate a high-quality dataset for further processing in IoT services [140]. Another approach is the use of a recruitment mechanism for selecting trustworthy users who are expected to contribute high-quality data. An appropriate recruitment scheme not only reduces system costs but also minimizes vulnerabilities, risks and potential attacks in MCS systems. Therefore using the proposed REK trust mechanism in a user recruitment mechanism in an MCS platform not only prevents adversaries from contributing falsified data and potential attacks but also motivates users to provide high-quality data in order to be recruited in the next sensing tasks, hence strengthening the MCS platform.

6.2 Background and Related Work on Mobile Crowd-Sensing

6.2.1. Mobile Crowd-Sensing in the IoT

In the IoT ecosystems, data from various sources such as actuations, sensors, and smart devices are gathered, analysed and processed to provide ubiquitous and intelligent services [141, 142]. In this environment, users could contribute to the progress of the IoT platform through sharing not only data sensed from their own devices' sensors but also their incidents and knowledge over social networks without the need to pre-allocate sensing devices in the area [143], hence saving deployment costs [144, 145]. This prospect coins the term MCS that has gained popularity as a promising data acquisition for the IoT because of the increasing usage of mobile smart devices. These devices are equipped with different types of sensors such as GPS, accelerometer, gyroscope, microphone and camera with advanced features including computation processing and wireless communications that can efficiently support crowd-sensing processes [146, 147]. In an MCS platform, heterogeneous information regarding different aspects of human life is collected from mobile devices before being aggregated, analysed and mined for supporting a variety of IoT applications and services (Figure 6-1).

With regards to the data acquisition models, an MCS system can be categorized as either opportunistic or participatory [137]. In optimistic sensing systems, data is automatically collected using a background process such as reporting speed and Global Positioning System (GPS) coordination while driving in navigation services. Sensing decisions are application or device-driven, meaning that the involvement of participants is minimal, thus, a user recruitment is not necessary. Conversely, in participatory sensing systems, participants agree to a requested sensing task that dispatches from an MCS centralized platform. Users are explicitly engaged in the sensing process by accepting or rejecting the sensing request; and by actively collecting data such as taking a picture, reporting an available parking lot and manually providing information. Such kinds of sensing data can be extracted and directly consumed by end-users for supporting some prompt services or further aggregated in the cloud for large-scale sensing and community intelligence mining [4].

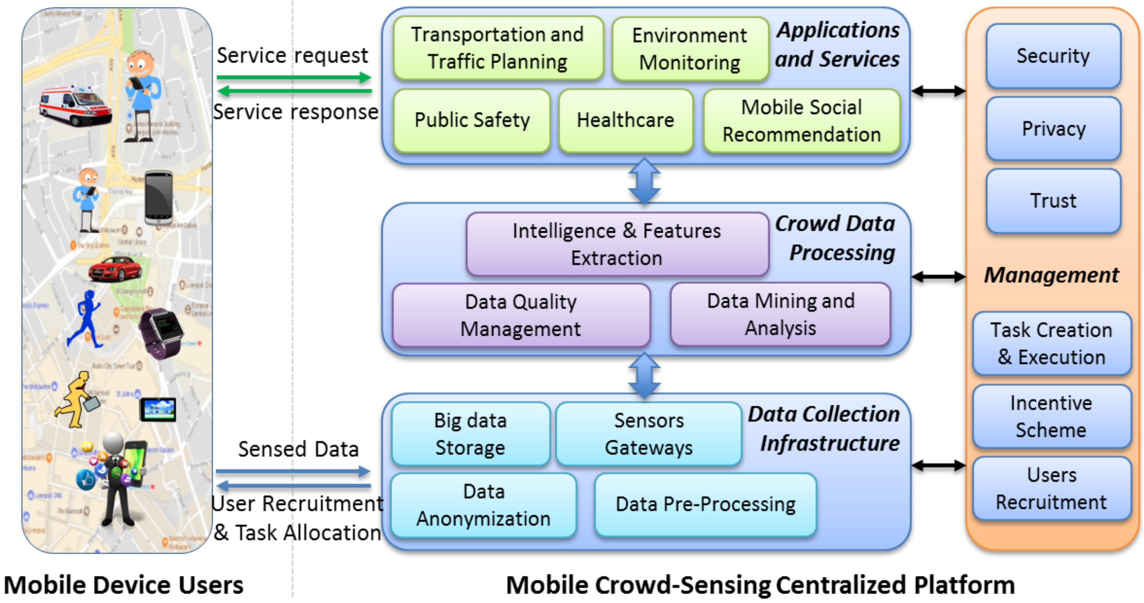


Figure 6-1. A Centralized MCS Platform Architecture

6.2.2. User Recruitment in Mobile Crowd-Sensing

Generally, a life cycle of an MCS system comprises of three phases: “task creation and user recruitment”, “task execution” and “data collection and processing” [148]. Zhang *et al.* have divided the life cycle into four phases: “task execution”, “task assignment”, “individual task execution” and “sensing data integration” [149]. The “task assignment” phase recruits users and assigns individual sensing tasks for these users. Nevertheless, the user recruitment scheme plays a key role in the success of any participatory MCS systems. The recruitment not only selects proper users for providing high-quality data but also allows MCS service providers to manage expenditure by considering incentive costs based on users’ contributions. These MCS systems are tailored to a centralized MCS platform illustrated in Figure 6-1, which facilitates major system control operations including the user recruitment for MCS systems.

Some user recruitment approaches in a centralized MCS platform have been investigated. Reddy *et al.* have proposed a mechanism that recruits participants based on the user availability, time and location[150]. Karaliopoulos *et al.* have used deterministic and stochastic mobility models for solving an optimization problem on cost minimization and user location in their recruitment policy[151]. Some researchers have employed piggyback crowd-sensing techniques that analyse information from users such as phone calls, GPS coordination, and application usages for predicting geographical coverage. As a result, such recruitment mechanisms are able to determine the minimum number of participants[152, 153], to find an energy-efficient strategy [154], or to bargain incentives with users (i.e., auction mechanism) for minimizing sensing costs [155]. Authors in [156] have proposed a recruitment policy based on statistics of social services usage to compute a “sociability” metric indicating the willingness of users to participate in sensing tasks. Such recruitment schemes aim at minimizing sensing costs for an MCS service provider while guaranteeing certain requirements of requested services such as sensing areas coverage. In these mechanisms, however, the data quality is neglected. There are multiple factors affecting the recruitment process, and the assurance of high-quality sensing data is of paramount importance.

6.2.3. Reputation-based User Recruitment Schemes

Recently, several efforts have been proposed to recruit users based not only on time, location and statistical metrics but also on reputation. Regular users and adversaries are assumed to behave differently; and reputation is as an indicator to perceive trustworthy participants in MCS sensing tasks. Following this trend, Kantarci *et al.* have proposed a reputation-based MCS management adopting the M-Sensing auction approach [157] in which a statistical reputation is taken into account [158]. The statistical reputation here is simple as the percentage of true sensor readings over total readings. Pouryazdan *et al.* have further employed a vote-based approach using a social network for evaluating users' reputation [159, 160]. In this platform, users who have already participated in a common sensing task during a recent time window form a community. All members of a community will vote on the reputation of a newly joining user based on their similarity on sensor readings.

Such reputation-based recruitment schemes use reputation on behalf of trust. Reputation is one of the TIs, that partially affects trust, but should not be confused with trust [100]. Moreover, the mechanisms are either too simple [158, 161] based only on statistical sensor readings, or impractical assumptions [159, 160]. For instance, if two users join in the same sensing task, then there will be an interaction between the two; and they will get connected and directly interact with each other. Another assumption is that any user has the right to access all previous readings of other users in the same community for making up their votes. This results in the unfeasible deployment of these mechanisms in the real world. Given the state-of-the-art, we propose a trust evaluation mechanism that can be effectively used to recruit trustworthy users while being practically deployed for the real-world services.

6.3 Knowledge-based Trust Analysis in Mobile Crowd-Sensing Systems

An efficient User Recruitment scheme implemented in the MCS Tasking Server is necessary for making a proper selection of contributors with respect to a specific sensing task as illustrated in Figure 6-2 (the sensing task requested by service providers and assigned based on a mechanism deployed at the MCS [162]). Note that in order to recruit users evolving in a sensing task, the MCS Tasking Server should manage an incentive scheme as rewards for their contributions because users sustain costs (e.g., energy consumption, data subscription, and privacy and security breach) for accomplishing assigned sensing tasks. The User

Recruitment scheme specifies criteria for user eligibility to contribute to a crowd-sensing campaign by judging whether a user accomplishes a sensing task as expected. In other words, the MCS Tasking Server chooses contributors it trusts to fulfil the sensing task. Therefore, this use-case turns to a trust scenario as follows:

Evaluate trust between the MCS Tasking Server (as the trustor) and owners of mobile devices (as the trustees), with respect to a sensing task (as the trust goal).

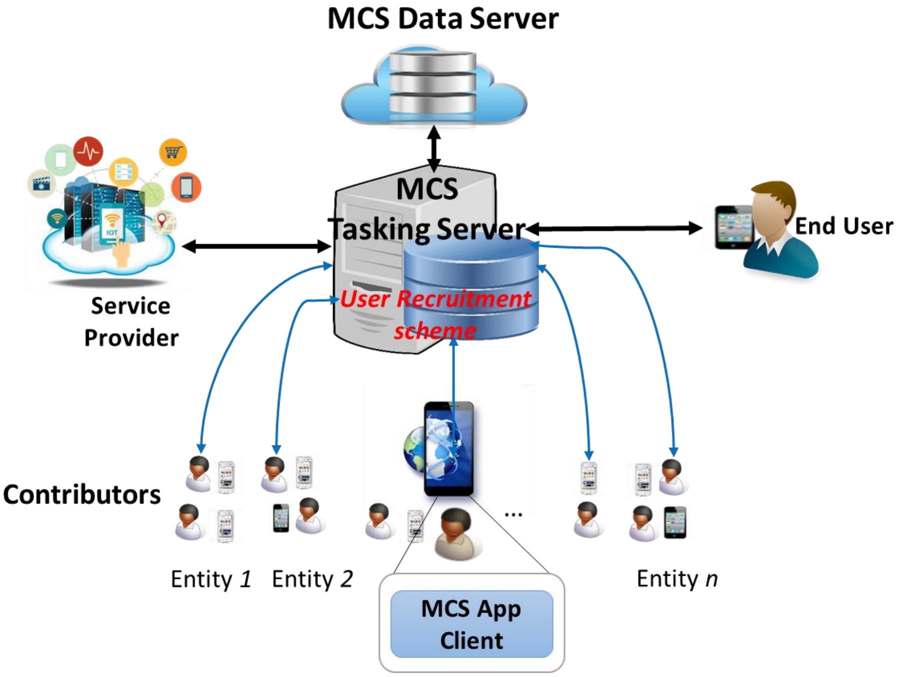


Figure 6-2. Mobile Crowd-Sensing System Architecture.

A sensing task called Traffic Congestion and Accident Report is considered as follows: Report accidents and traffic congestion at a specific crossroad X. The sensing task is event-based, spatial, urgent, and nearly real-time required. Contributors should report the situation of the traffic at the crossroad X by sending data obtained from smartphone sensors such as accelerometer, magnetometer, and GPS coordinates as well as submitting an image or a video about the traffic incident [163, 164]. Based on the proposed Knowledge TI model, a set of TAs is deliberately chosen as following:

- **Spatial Distance:**

This TA shows the distance between a contributor and the crossroad X. The contributor should be close enough to the crossroad X so that it is able to report traffic situation correctly to the MCS server. The distance can be calculated based on the GPS coordinates of the smartphone and the crossroad X using the "*haversine*" formula presented in [165]. This TA belongs to the Ability dimension and should not exceed the distance boundary (as a threshold).

- **Availability:**

Availability is a TA indicating the activeness of a user in getting connected to social activities. It shows how much a user uses his smart device for social applications and is ready to fulfil an assigned task which is essential to consider for user recruitment. The Availability can be calculated based on both time spent on social network applications and amount of data consumed [166, 167]. This TA belongs to the Ability dimension.

- **Transmission Capability:**

It is required to be reliable, fast, and secure when fulfilling important tasks in traffic incident reports; thus this indicator is essential for reflecting the capability of a smart device to transmit data in real-time or nearly real-time as well as in a secure and private manner without compromise. Therefore, this indicator includes several TAs in the Ability dimension mentioned in Section 4.2.1 such as Reliability, Confidentiality and Integrity. For simplicity, we specify the level of the Transmission Capability based on some information: signal strength, signal-to-interference-plus-noise-ratio (SIRN), and the communication technology in use (WiFi, LTE, 3G, WiMax, and Bluetooth). For example, Transmission Capability is high when the user is using 4G LTE for data transmission with high signal strength (4G LTE Signal ≥ -50 dBm) and high LTE SIRN (LTE SIRN ≥ 12.5) whereas it is low when 3G is used with low 3G SIRN (3G SIRN ≤ -5).

- **Cooperativeness:**

This TA represents the degree to which a user cooperates with crowd-sensing tasks, thus, high cooperativeness indicates more opportunities that the user is willing to accomplish an assigned sensing task, and vice versa. This TA belongs to the Benevolence dimension. Cooperativeness can be simply calculated by using the following equation:

$$Cooperativeness(i) = Frequency(i) \times \frac{|Number\ of\ tasks\ involved\ |}{|Number\ of\ tasks\ requested\ |} \tag{6-1}$$

where $Frequency(i)$ indicates how frequently the *user i* has been involved in the crowd-sensing campaign. It is calculated based on the following equation:

$$Frequency(i) = \frac{|Number\ of\ sensing\ tasks\ involved|}{|sampling\ period\ of\ time|} \tag{6-2}$$

The numbers of tasks requested is the number of times the MCS Tasking server has requested the user to participate in a sensing task; and the number of tasks involved is the number of times the user has accepted to be involved in sensing tasks that the MCS has requested. The number of tasks cancelled is the number of times the user cancels a sensing task when it has already accepted to be involved in the sensing task. The number of requested, involved, and cancelled sensing tasks of the user i is kept track of and managed by the MCS Tasking Server.

- **Honesty:**

This TA represents the degree of keeping a promise once a sensing task is already assigned to a user. High honesty means that the user is not going to cancel a task once it is assigned for any reason whatsoever. This TA belongs to the Integrity dimension and it is simply measured by the following equation:

$$Honesty(i) = 1 - \frac{|Number\ of\ tasks\ canceled|}{|Number\ of\ tasks\ involved|} \tag{6-3}$$

Mechanisms for inferring the direct trust Knowledge TI from the considering TAs have already been introduced in CHAPTER 5. For instance, the weighted sum method can be used for simply aggregating the set of TAs mentioned above. The Knowledge TI might be combined with the two Experience and Reputation TIs which are described in the next sections in this chapter for strengthening the evaluation of trust in the MCS scenarios.

6.4 Experience and Reputation-based Trust Evaluation in Mobile Crowd-Sensing Systems

In this section, we propose a novel mechanism for evaluating trust relationships between service requesters and data contributors. To establish and evaluate the trust relationships, the Reputation-Experience-Knowledge (REK) trust model, which comprises of the three concepts of TIs called Reputation, Experience and Knowledge, is utilized [100, 168]. To employ the REK mechanism, virtual interactions between service requesters and data contributors are established and managed. The virtual interactions are formed when a user requests a service, then other users contribute their sensing data to fulfil the service. The interactions are then quantified by performing QoD assessment over the contributed data. Based on the interactions, Experience between service requesters and data contributors is generated and updated. Standing on the Experience relationships among users in MCS systems, Reputation for users is calculated accordingly. Trust relationships between users are finalized by combining the two associated TIs; Experience and Reputation. As a result, the proposed trust-based recruitment scheme simply examines trust relationships between a service requester and potential participants for selecting trustworthy data contributors for a requested service.

To verify the effectiveness of the trust-based recruitment scheme, a quality of service (QoS) evaluation model for an MCS service based on QoD assessment of collected data is also proposed. We simulate the trust-based recruitment mechanism along with two popular predictive schemes based on QoD assessment in the same

MCS testbed for comparisons. The results indicate that the trust-based scheme not only provides better QoS for MCS services but also efficiently differentiates between high-quality, low-quality and malicious users.

6.4.1. E-R Trust Mechanism in MCS Platform

This section explores an MCS system model, scenarios and introduces the E-R trust mechanism and its components deployed on top of a centralized MCS platform.

6.4.1.1.MCS System Model and Scenarios

In an MCS platform, users share and provide data from their smart devices through being physically close (direct sensing model) or through a centralized MCS platform (indirect sensing model) [169]. In the direct sensing model, direct interactions exist between a requester and provider in which sensing data is transmitted in a peer-to-peer manner. This sensing model uses a variety of wireless communication technologies such as Wi-Fi direct, ZigBee, Near-Field Communication (NFC) and Bluetooth over a social platform that operates among nearby smart devices' users [170, 171]. In the indirect sensing model, a requester and a provider indirectly interact over a centralized MCS platform. In this model, users can upload and obtain data to and from a cloud server through wide-range communication technologies such as WiFi, WiMax and 3G/4G LTE. The indirect sensing model adopts the well-known service-oriented approach model called Sensing as a Service (SaaS) [172]. Melino *et al.* have further developed a Cloud-based SaaS designated for MCS systems called Mobile Crowd-Sensing as a Service (MCSaaS) [173].

Nevertheless, in any MCS models, a user can be either a "requester" that asks for a service or a "data provider" that collects and delivers data being used by another service; thus MCS users are directly or indirectly interacting with each other. This introduces either a "direct" or an "indirect" relationship between a "service requester" and a "data provider" depending on the sensing model deployed in an MCS system. In this chapter, we consider MCS systems that adopt the indirect sensing model with participatory data acquisition style, which are overwhelming in the real-world usage. For such a system model, there is a centralized MCS cloud platform that handles and operates all the MCS processes including data collection and processing, task creations and execution; and the user recruitment and incentive schemes as illustrated in Figure 6-1.

6.4.1.2.E-R Trust Mechanism in the MCS Platform

Trust can be considered as 'belief' of a trustor in a trustee that the trustee will perform a task as the trustor's expectation. Trust plays an important role in supporting participants to overcome perception of uncertainty and risks when making a decision [100]. In the MCS context, trust can be utilized to predict whether a mobile device user (i.e., the trustee) is going to provide high-quality data for a service requested by a service requester (i.e., the trustor). To establish and evaluate trust relationships between service requesters and data contributors, the REK trust model proposed in [94, 100, 168] is employed.

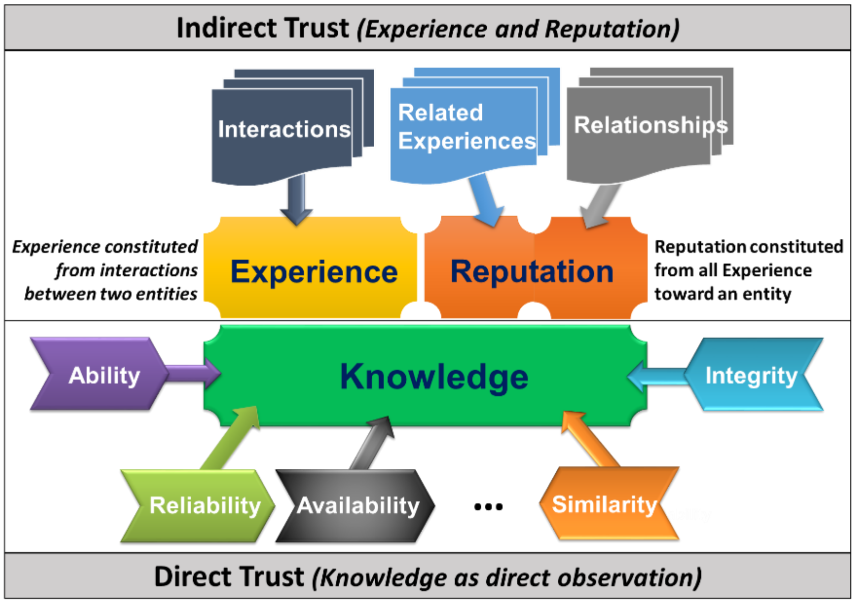

Indirect Trust (Experience and Reputation)
Interactions
Related Experiences
Relationships
Experience constituted from interactions between two entities
Experience
Reputation
Reputation constituted from all Experience toward an entity
Ability
Knowledge
Integrity
Reliability
Availability
...
Similarity
Direct Trust (Knowledge as direct observation)

Figure 6-3. Trust Indicators and Attributes in the REK Trust Model

As depicted in Figure 6-3, trust is comprised of three TIs called Reputation, Experience and Knowledge. Knowledge is as “direct trust” and evaluated by inferring trustees’ characteristics considering the trust context [100]. In the MCS context, Knowledge is constituted from a variety of attributes such as availability, mobility model, GPS coordination and geography coverage. These attributes specify criteria for user ability and eligibility for fulfilling crowd-sensing campaigns. Experience and Reputation are “indirect trust” quantified by accumulating previous interactions between mobile device users. Experience is a relationship between two users reflecting the personal perception of a trustor on a trustee. Reputation is a property of a user indicating the global consciousness of the user by considering all personal perceptions towards it [100].

Knowledge assessment requires various information from mobile device users that impose critical privacy concerns. Moreover, some information is a challenge to retrieve which is not practical to implement in real-world scenarios [100]. For those reasons, we simplify the REK model called E-R that relies only on two indicators; Experience and Reputation. Knowledge is neglected in the E-R model, but some information could play as supplemental factors in strengthening the evaluation of trust. As illustrated in Figure 6-4, the E-R trust component is integrated in a centralized MCS cloud platform that establishes and manages virtual interactions between mobile-device users. An indirect interaction occurs after each sensing task is accomplished; and the interaction value is calculated based on QoD provided to the MCS system (from data providers) and feedback (from service consumers). Experience between any two users is established and updated by an aggregation model on the virtual interactions. Based on all Experiences between users, Reputation of each user is calculated accordingly. Finally, the value of a trust relationship is calculated by aggregating Experience and Reputation. Detailed calculation models for Experience, Reputation and trust value are presented in previous sections.

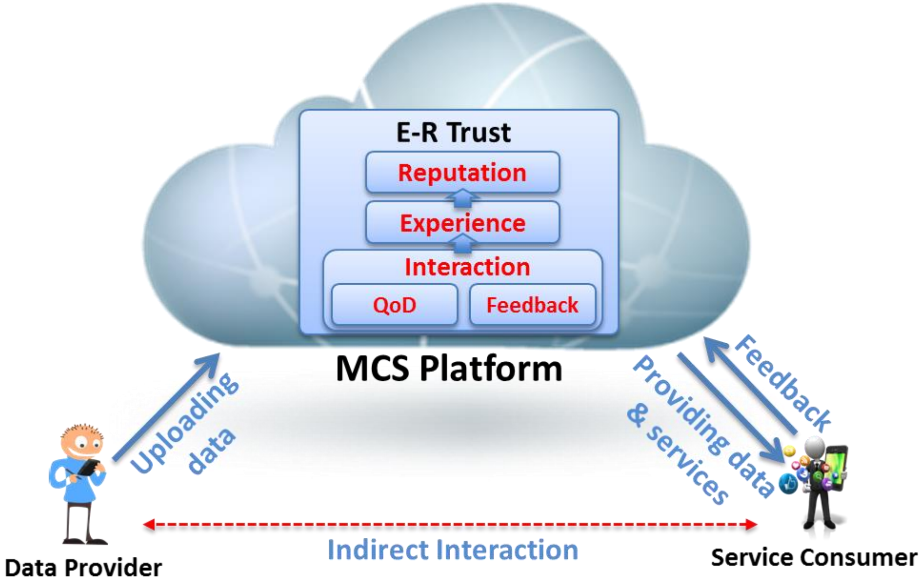


Figure 6-4. E-R Trust Mechanism in the centralized MCS platform

6.4.1.3.Quality of Data Assessment

The target of MCS systems is to extract useful knowledge and intelligence from sensing data for delivering smart services; and to achieve this aim, high quality of data must be ensured [174]. Low-quality data might cause numerous problems such as deception in decision making, consumer dissatisfaction and distrusting the system [175]. Well-known research works have pointed out that QoD consists of some dimensions as measurable properties representing some aspects of data illustrating the data quality [176, 177]. Certain data can be identified as high quality based on the measurements of multiple dimensions [175]. The six data quality dimensions as specified by Askham et al. in [176] have been widely accepted, namely Accuracy, Completeness, Consistency, Timeliness, Uniqueness, and Validity. Detailed analysis and measurement methodologies for the six dimensions have been also proposed in related articles. Based on system requirements, context and system goals, certain dimensions can be taken into consideration for the QoD assessment [178, 179].

We have utilized QoD calculation mechanisms in [176] [177] for measuring QoD of live data streaming from traffic sensors and parking sensors deployed in Santander City Centre, Spain as a result of the Wise-IoT[5] project. As the data is presented in semantic form, we have proposed two novel dimensions called Syntactic Accuracy and Semantic Accuracy in the QoD assessment [180]. The two dimensions are suitable for checking data syntax and semantics from live information produced by the sensors (Figure 6-5) using predefined data quality rules as well as the ontology validating rules developed by EGM partner[6] [180]. We believe this mechanism can be perfectly used for evaluating sensing data in an MCS platform because the underlying theoretical and practical QoD assessments are identical.

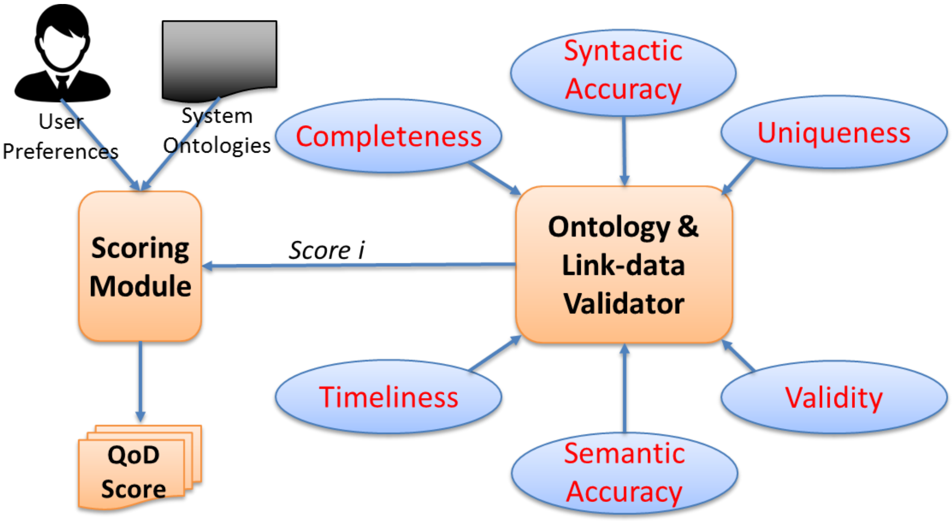


Figure 6-5. QoD Monitoring Module for traffic and parking sensors in the Wise-IoT project

6.4.1.4.User Feedback

QoD is an important indicator of how contributors fulfil assigned sensing tasks, but it might not be enough. QoD scores do not completely reflect the level of consumers' satisfaction with service providers. In this regard, feedback could complement the assessment of to what extent a service provider has accomplished a requested service. Feedback can be both implicit and explicit; and may or may not require human participation [181]. Feedback could be obtained by directly asking customers to give opinions after a service has been provided. This approach has been used in many e-commerce services such as eBay, Amazon and Airbnb, which requires huge effort to attract users to participate; and opinions are sometimes biased. The second approach is based on calculation models with some predefined criteria to estimate the outcome which normally does not require a human participant. It has been applied in some networking protocols as an ACK message to indicate whether a packet or a file is transmitted successfully or unsuccessfully [6, 16].

[5] http://wise-iot.eu/en/home/
[6] http://www.eglobalmark.com/

User feedback is out of scope of this section. In the E-R trust component, we neglect the feedback mechanism, thus indirect interactions between users rely on QoD scores only. However, user feedback could be an essential component for improving quality of IoT services; thus, it is worth being introduced.

6.4.2. E-R Trust Evaluation Mechanism

In this section, the mathematical calculation models for the E-R trust mechanism are described in detail.

6.4.2.1.Experience Model

Experience is an asymmetric relationship between two entities built up from previous interactions reflecting to what extent a trustor trusts a trustee. After each interaction, awareness between the trustor and the trustee is supposed to get better, and Experience should be maintained and correctly indicate the relationship between the two (Figure 6-6). The proposed Experience model in MCS systems follows human relationships investigated in sociological literature [119, 120] as already presented in Section 5.3 as following:

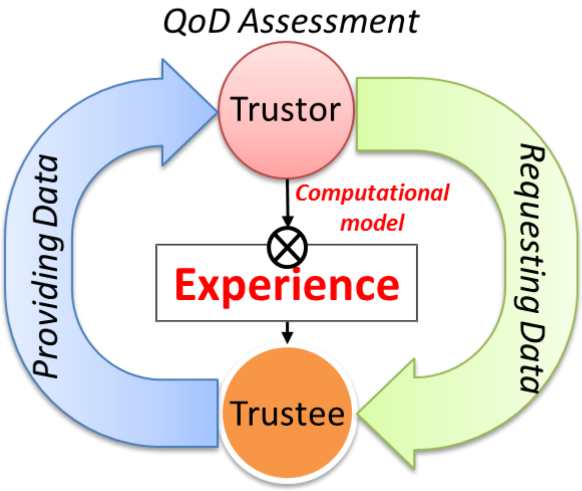


Figure 6-6. Experience Model based on QoD Assessment in MCS platform

- **Increase (due to cooperative interactions)**

  Let ϑ is the QoD score, normalized in the range [0, 1]. A cooperative interaction is when $\vartheta > \theta_{co}$ threshold. The increase is modelled using a linear difference equation as mentioned in Section 5.3:

$$Exp_{t+1} = Exp_t + \vartheta_t \times \Delta Exp_{t+1} \tag{6-4}$$

$$\Delta Exp_{t+1} = \alpha \times (1 - \frac{Exp_t}{max_{Exp}}) \tag{6-5}$$

  Experience accumulates from cooperative interactions and accumulated values depend on both QoD score ϑ_t and the current value Exp_t.

- **Decrease (due to uncooperative interactions)**

  An uncooperative interaction is when the QoD score $\vartheta < \theta_{unco}$ threshold. The Decrease model is as follows:

$$Exp_{t+1} = Max\langle min_{Exp}, Exp_t - (1 - \vartheta_t) \times \beta \times \Delta Exp_{t+1} \rangle \tag{6-6}$$

- **Decay (due to no interactions or neutral interactions)**

$$Exp_{t+1} = Max\langle init_{Exp}, Exp_t - \Delta decay_{t+1} \rangle \tag{6-7}$$

$$\Delta decay_{t+1} = \delta \times \left(1 + \gamma - \frac{Exp_{t-1}}{max_{Exp}}\right) \tag{6-8}$$

6.4.2.2.Reputation Model

Reputation is a property of a mobile device user reflecting the overall opinion of a community about the user. In the MCS environment, especially in urban scenarios with a large number of mobile users, only a small number of users have already interacted with others, resulting in very high possibility that a service requester and a data provider are new to each other, thus there is no prior experience between the two. Reputation therefore is a vital indicator for the trust evaluation. The Reputation model in this case is same as the model proposed in 5.4 as follows:

- **Positive Reputation:**

$$Rep_{Pos}(U) = \frac{1-d}{N} + d \times \left(\sum_{\forall i} Rep_{Pos}(i) \times \frac{Exp(i,U)}{C_{Pos}(i)}\right) \tag{6-9}$$

  where: $C_{Pos}(i) = \sum_{Exp(i,j)>\theta} Exp(i,j)$ is the sum of all positive Experience from the user i.

- **Negative Reputation:**

$$Rep_{Neg}(U) = \frac{1-d}{N} + d \times \left(\sum_{\forall i} Rep_{Neg}(i) \times \frac{1 - Exp(i,U)}{C_{Neg}(i)}\right) \tag{6-10}$$

  where: $C_{Neg}(i) = \sum_{Exp(i,j)<\theta}(1 - \ Exp(i,j))$ is the sum of all compliment of negative Experience from the user i.

  Overall Reputation: combining of two positive and negative reputations

$$Rep(A) = \max\left(0, Rep_{Pos}(U) - Rep_{Neg}(U)\right) \quad (6\text{-}11)$$

where N is the number of users in a MCS system and d is the damping factor (is normally set to 0.85).

- **Finalize Trust Value**

  A trust value is an aggregation of the Experience and Reputation values. A simple weighted sum for calculating a final trust value between trustor A and trustee B is used as following:

$$Trust(A,B) = \alpha Rep(B) + \beta Exp(A,B) \quad (6\text{-}12)$$

where $\alpha, \beta > 0$ are weighting factors satisfying $\alpha + \beta = 1$.

6.4.3. Simulation Testbed and User Recruitment Schemes

This section describes a MCS testbed in which the trust-based user recruitment along with other two recruitment schemes based on Average and Polynomial Regression predictive models [182] are simulated.

6.4.3.1.User Models in MCS

Some statistics and analysis on the QoD of the real stream of data collected from traffic sensors[7] and parking sensors[8] deployed in the city of Santander, Spain in the Wise-IoT project are carried out. The histograms of QoD from reliable sensors, low-quality sensors and defective sensors are analysed normalized in the range (0, 1). Based on such a histogram, we have observed that QoD scores distribution from any sensor nicely fits to the Beta probability distribution family. And by using a Beta parameter estimation mechanism, we categorise users in an MCS system into three groups based on their QoD scores distribution called High-quality Users, Low-quality Users and Malicious Users. Detailed information for the QoD distribution of the user categories is in APPENDIX A: 2.

6.4.3.2.QoS Evaluation Model for MCS Services

To evaluate and compare the effectiveness between different user recruitment schemes in the performance of MCS services, a QoS evaluation model is proposed. Low-quality data lowers system efficiency and misleads system operations that directly leads to customer dissatisfaction [183]. Low-quality data also increases system operational overheads and cost; as well as imposing vulnerabilities and risks on the systems [184]. Some QoS evaluation models for IoT services have been proposed, taking into

[7] https://mu.tlmat.unican.es:8443/v2/entities?limit=1&type=ParkingSpot

[8] https://mu.tlmat.unican.es:8443/v2/entities?limit=1&type=TrafficFlowObserved

consideration different factors at various layers from the IoT infrastructure [185]; and QoD is one of the pivotal factors in the evaluation of QoS for MCS services.

Considering a service request R that comprises of T sensing tasks $ST_R(i); i = \overline{1, T}$; each sensing task $ST_R(i)$ is fulfilled by Pi participants providing Pi datasets with $QoD_{ST_R(i)}(j); j = \overline{1, P_i}$, respectively. The QoS for the service R is calculated as follows:

$$QoS(request\ R) = \frac{T}{\left|\log\left(\prod_{i=1}^{T} QoD_{ST_R(i)}\right)\right|} \tag{6-14}$$

$$QoD_{ST_R(i)} = \frac{\sum_{j=1}^{P_i} QoD_{ST_R(i)}(j)}{P_i} \tag{6-15}$$

Equation (11) depicts that the QoS of the service request R is proportional to the QoD scores of each sensing task $QoD_{ST_R(i)}$; $i = \overline{1, T}$, represented by the product of the natural logarithm of these scores. The $QoD_{ST_R(i)}$ score of the sensing task $ST_R(i)$ is calculated by taking average of the QoD scores from the P_i contributors associated to the sensing task. This is because contributors in the same sensing task are normally required to collect the same sort of data; such redundant datasets are then filtered and pre-processed to retrieve a high-quality dataset before processing and mining. However, the number of participants in each sensing task should be small enough in order not to incur much computation and storage overhead. Nevertheless, user recruitment plays a crucial role in providing high-quality services because even though a sensing task fulfilled by many participants, some attackers providing extremely low QoD could result in massive damage to the MCS services.

6.4.3.3.Trust-based, Average, and Polynomial Regression User Recruitment Schemes

Generally, the three recruitment schemes have the same purpose of recruiting mobile device users that are expected to provide high QoS scores for sensing tasks of an MCS service request. The algorithms to recruit users in the three schemes rely only on QoD scores of sensing data contributed by users who have been recruited in previous sensing tasks. The Trust-based recruitment scheme uses trust relationships between a service requester and other users for recruiting participants. The Average-QoD and Polynomial Regression-QoD schemes use the two popular predictive schemes; namely Average and Polynomial Regression, respectively, for predicting the QoD scores, then recruit users who are likely to provide highest QoD scores for the next sensing task accordingly. The three algorithms are demonstrated in the mathematical-style pseudo-code can be found in APPENDIX A: 3.

6.4.4. Simulation Results and Discussions

The testbed is implemented in Matlab containing of a set of users consisting of low-quality, high-quality and malicious users, a number of service requests, and the three user recruitment schemes. For comparison purposes, all three schemes take the same inputs (i.e., set of users and the service request) and produce output as the QoS of the service after a number of sensing tasks. The source code of the implementation can be found here[9].

6.4.4.1.Parameters Settings

- **Experience Model**

  Experience model is simulated with parameters settings shown in Table 6-1. Note that different real-world use-cases might result in different parameter settings.

TABLE 6-1. PARAMETERS SETTINGS FOR THE EXPERIENCE MODEL

Parameters	Values	Parameters	Values
max_{Exp}	1	γ	0.005
min_{Exp}	0	δ	0.005
$init_{Exp}$	0.3	θ_{unco}	0.3
α	0.1	θ_{co}	0.6
β	2		

- **Reputation Model**

  Reputation mechanism in an MCS system can be calculated either algebraically or iteratively. The algebra traditional method to solve the matrix equations (6) and (7) takes roughly N^3 operations that is not suitable for a large number of users (N is the network size, i.e., the number of users). On the other hand, the iterative method is much faster because the Rep_{Pos} and Rep_{Neg}vectors converge after conducting a number of iterations [129]. We use the second method in this simulation with the *error_tolerance* = 10^{-3} and the number of users is from 200 to 1000 and it takes from 25 to 32 iterations to converge. This reputation calculation is suitable for huge networks like the IoT as the scaling factor is roughly linear in logarithm of N [168, 186].

- **Testbed simulation scenarios**

  The number of service requests is varied from 1 to 160, and without the loss of generality, we assume that each service request is fulfilled by a random number of sensing tasks from 5 to 15. Each sensing task requires a number of users from 5 to 200 (50% of the total users). The total number of users N is set at

[9] https://github.com/nguyentb/MCS_project

400; and the number of malicious users is varied from 0% to 25% of N. We also assume that a user can participate in several tasks simultaneously.

6.4.4.2.Results and Discussion

We implement the Trust-based scheme with the other two algorithms. For better observation, we also implement a random selection method as the simplest recruitment scheme. As can be seen in Figure 6-7, the Trust-based scheme outperforms all other schemes in most of the cases, meaning that the quality of requested services using the proposed trust-based user recruitment is better than the other schemes. All of the schemes, except the Random Selection, are getting better QoS scores as more requested services are served. However, just after a period of about 15 requests (i.e., learning phase), the Trust-based scheme achieves consistent QoS scores for the next services whereas the Average-based and the Polynomial Regression take about 35 and 70 requests, respectively. After the learning phase, the Trust-based scheme persistently achieves the highest QoS scores compared to the other schemes, at about 3.35 to 3.55 QoS scores from the Average-based scheme fluctuated between 3.10 and 3.35 while the Regression outcomes steadily increase and reach about 3.25 to 3.40.

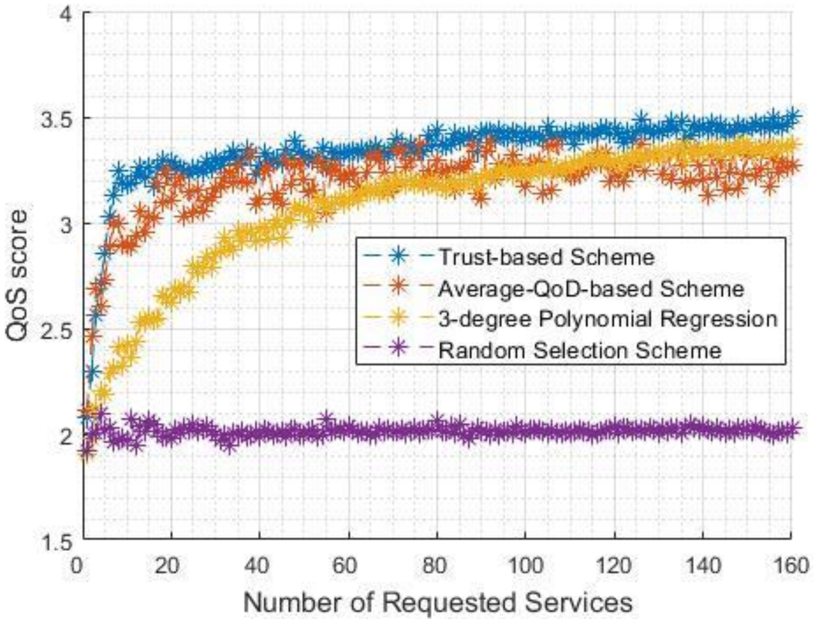


Figure 6-7. QoS scores after numbers of services using different User Recruitment schemes

The three schemes can learn from previous data contributors for maximizing the outcomes. However, except the Trust-based scheme, the other schemes fail to detect malicious users. That is why some malicious users are still recruited in these schemes resulting in lowering down the QoS scores for requested services. This is understandable because the Average-based scheme considers malicious users as high-quality users due to the fact that the average QoD scores from these users are similar. Compared to the Average-based scheme, the Regression method produces just slightly better QoS and is more consistent after a long learning phase. This is because malicious users contribute high-quality data for most of the time so that low-quality data, which rarely incurs, could be considered as outliers in the regression model. This is why some malicious users are quantified as high-quality users. The regression model also requires more data points for more accurate prediction resulting in the long learning phase.

Unlike these two, the Experience model heavily penalizes a user who sometimes produces very low QoD scores, resulting in dropping down the trust relationships and reputation value of the users. By looking at the reputation vector for all users after the learning phase, we figure out that reputation values of malicious users are normally lower than low-quality users and far lower than high-quality users. That is why after the learning phase, the trust-based scheme can avoid recruiting malicious users.

We also examine some scenarios in which the number of malicious users is varied. Figure 6-8 shows that as the percentage of malicious users over total users is increased, the QoS is decreased. This is inevitable because the possibility to recruit malicious users is getting higher. However, as the number of requested services increase, QoS scores from all schemes, except the Random Selection, get higher. For instance, at 15% of malicious users, the QoS scores from the Trust-based scheme are increased to about 3.2, 3.35, 3.5 and 3.6 after serving 10, 40, 80 and 160 services, respectively. As can be seen in Figure 6-8, as the number of malicious users increase, the gap of QoS scores between the Trust-based scheme and the others gets expanded, especially as more requested services are accomplished, showing the advantages of the Trust-based scheme in risky environments. For example, at 10% and 25% malicious users after 160 requested services, the difference of QoS scores obtained from the Trust-based scheme and the Regression scheme increases from 0.07 to 0.18. If the percentage of malicious users is less than 10%, then the Average-based scheme is the best option that offers similar QoS scores but requires less computing resources. Unlike the Experience model, the Reputation model requires much more computational resources. Thus, it is not necessary to execute the reputation mechanism in every evaluation of trust. Instead, it should be periodically performed which could massively save time and computational resources

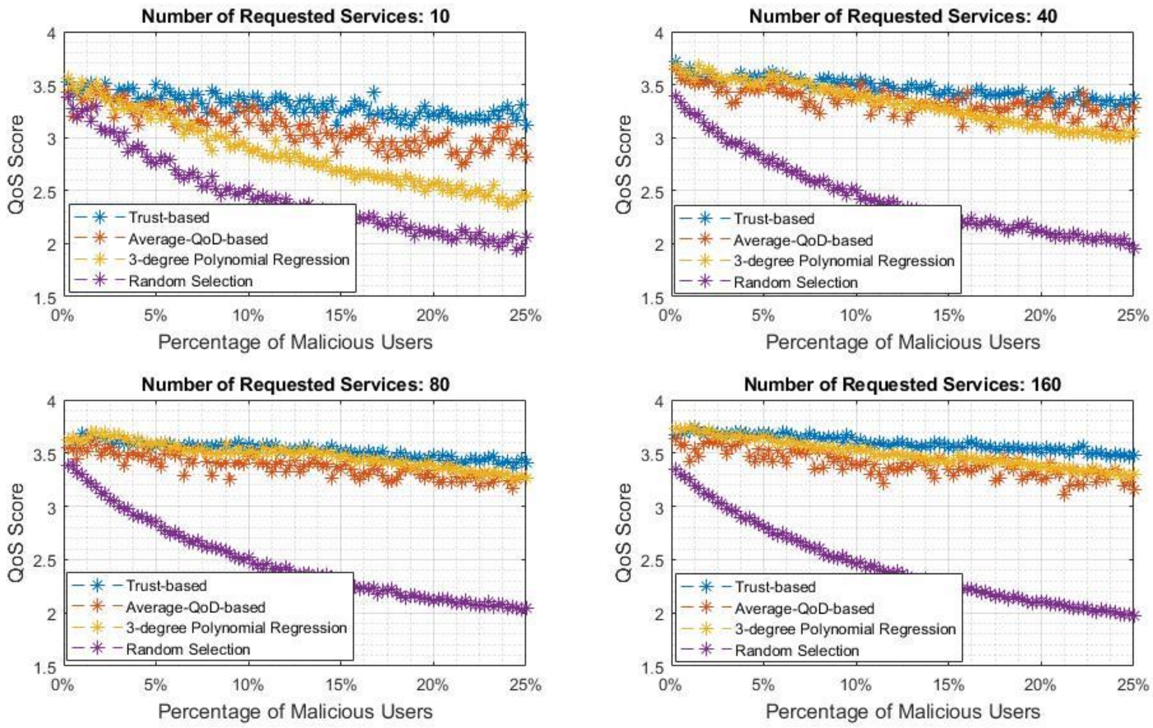


Figure 6-8. QoS scores in different Percentages of Malicious Users using different User Recruitment Schemes

6.5 Chapter Summary

In this section, we propose a trust evaluation mechanism along with a trust-based user recruitment scheme in an MCS platform in the IoT. To establish and manage trust relationships between mobile device users, we introduce a concept of virtual interactions in a centralized MCS platform, forming when a user contributes data for a sensing task from a requested service. The interactions are then quantified using the assessment of quality of contributed data; and being used as inputs for the proposed E-R trust evaluation mechanism. The E-R mechanism utilizes the REK trust model by considering two indicators of trust called Experience and Reputation. The mathematical model and simulation in an MCS testbed for the E-R mechanism are presented. The trust-based user recruitment scheme along with two other recruitment algorithms are also simulated in an MCS testbed for comparisons. The results reveal that the trust-based mechanism outperforms other schemes as providing better QoS for MCS services in most of the cases. It is also able to envisage different types of users including intelligent malicious users. The proposed user recruitment scheme is also practically implemented in real-world IoT services as we have been doing in the Wise-IoT project, which is better by far than other related recruitment mechanisms relying on unrealistic assumptions. This chapter opens some future research directions. The first direction is the automatic adaptation of parameter settings for the Experience and Reputation models in a context-aware manner. Different MCS systems have different characteristics and types of users which require to be examined, meaning that the QoD assessment, the user models and the QoS evaluation model could be different. This opens another research direction for customizing the proposed mechanism for specific MCS use-cases. The third direction is the integration of Knowledge, which contains various useful pieces of information of MCS systems, in the evaluation of trust, resulting in better selection of users.

CHAPTER 7. UTILIZE REK TRUST EVALUATION IN OTHER USE-CASES

7.1 Introduction

The proposed REK Trust Model is also applied in a variety of other applications and scenarios such as Car Sharing service, Data Sharing and Exchange platform in Smart Cities and in Vehicular Networks using Fuzzy Logics and Reasoning and Inference Engine technologies; and also for strengthening Blockchain-based systems in the Internet of Value. The feasibility and effectiveness of the REK model and associated evaluation mechanisms are proved not only by the theoretical analysis but also by real-world applications deployed in our ongoing TII and Wise-IoT projects.

This section describes in details the scenarios and applications that the proposed REK trust evaluation model is applied including use-case specific mechanisms and technical details. More information such as explanations and source code are also presented in the Appendix A and B.

7.2 Knowledge-based Trust Evaluation using Fuzzy Logic in Car Sharing

In this section, we take the trust-car sharing example for illustrating the policy mechanism reasoner. Generally, the Reputation and Recommendation TIs in the trust car-sharing example are similar to any other services; and can be got from the reputation system. We concentrate on how to evaluate Knowledge in this use-case. Car-sharing is a car rental model that people rent cars for short periods from others. The cars rentals could be a commercial business or individuals who want to rent their spare cars. Thus, it is attractive to both customers and providers who occasional use of a vehicle. The principle of car-sharing is that individuals gain the benefits of private cars without the costs and responsibilities of ownership[10]. However, currently there is no car-sharing mechanism that helps customers to choose car as they wish, except feedback ratings. Generally, customers tentatively want to rent a car that they trust the most, not only based on other feedback opinions but also based on each situation, their own knowledge of the vehicle and the vehicle owner. By using our trust service platform, the car-sharing service can show a customer a list of car sorted by the trust level based on customer's preferences.

Knowledge is the first party information provided by a trustee to evaluate its trustworthiness [187] and composed by some TAs depending on services and entities. Service providers are supposed to register their own information including both Knowledge TI ontology and requirements to the platform prior to use. This

[10] https://en.wikipedia.org/wiki/Carsharing

trust data has many dimensions and should be normalized and unified in order to be suitable for the software oriented architecture (SOA) environment by using an ontology manager and an information model. In this section we consider our platform is for service-to-service IoT environment in which humans offer services through their owned items. Thus, when judging Knowledge TI of a service, a user needs to assess both device and device's owner as illustrated in Figure 7-1. The Human-to-Human knowledge is comprised of four TAs: Honesty, Cooperation, Community-Interest and Experience, inspired by ideas in [188, 189].

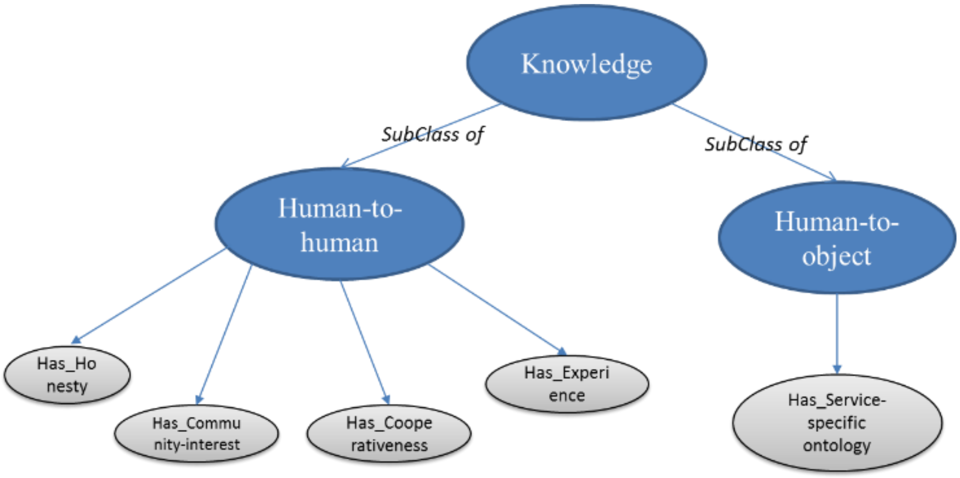


Figure 7-1. The Knowledge TI is divided into two sub-ontologies

- The honesty represents whether an entity is honest. In IoT, an entity can be dishonest when providing services or trust-related information that leads to disrupting the service continuity including trust management. Thus, honesty is chosen as a TA to prevent an entity from trusted-related attacks.
- The cooperativeness represents the level of the social cooperation from the trustee to the trustor. The higher cooperativeness means the higher trust level in the IoT system. The cooperativeness of an entity can be evaluated based on its social relations and its social behaviours.
- The community-interest represents whether two entities have a close relationship in terms of social communities, groups, and capabilities. A higher degree of community-interest can lead to high opportunities to interact with each other, resulting in higher trust level.
- The experience from one entity to another entity represents how well they previously interacted with each other. If a previous interaction is successful then, experience value is +1; or -1 if failure. A high value of experience can result in a high level of trust judgment.

The detailed calculations of the three TAs Honesty, Cooperativeness and Community-Interest are presented in [189] whereas the Experience TA is achieved from the interaction record conducted by the Trust Agent. By considering these TAs, our proposed trust service platform is able to deal effectively with several types of misbehaviour entities and attacks [39, 189]. The Human-to-Object knowledge depends on both service and object; and can be calculated using sufficient information provided from the service with appropriate reasoning methods and machine learning technique. This process will be clarified in the car-sharing use case in the next section.

7.2.1. Trust Analysis and Evaluation Mechanism

Fuzzy-based Policy Mechanism for Knowledge TI

As the trust platform perspective, Human-to-Object, in this case is Human-to-Vehicle, ontology and vehicle data are provided by the car-sharing service and users. We propose that the ontology is comprised of three TAs: Reliability, Pricing and Quality as depicted in Figure 7-2. To identify these TAs, it is crucial to explore what information is necessary and sufficient; and this process is a service level agreement between the trust platform, services and users. For example, vehicle owners are asked to show the sub-TI Reliability by supplying the maintenance schedule of their vehicles, the vehicle accident history or the insurance policy Figure 7-2.

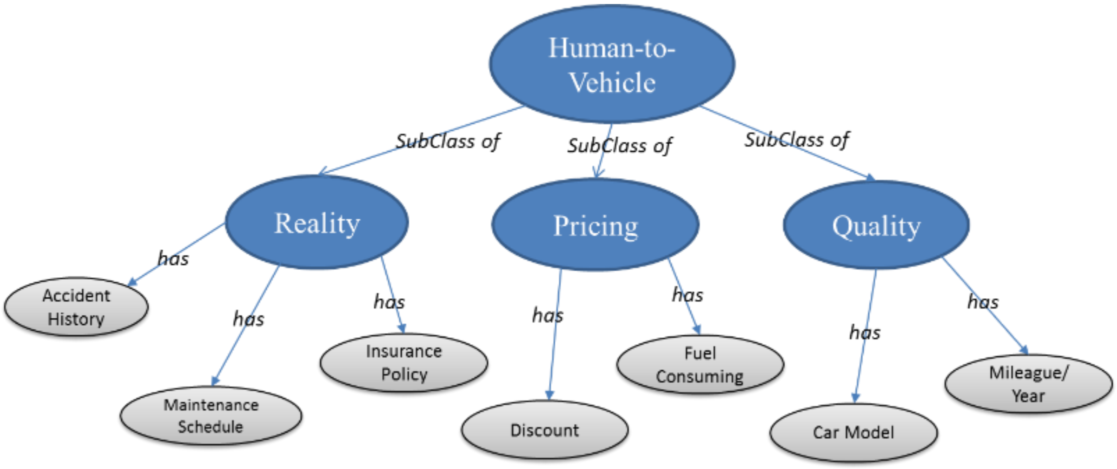


Figure 7-2.Knowledge in Human-to-Vehicle of trusted car sharing service

To deal with a wide range data of the Knowledge components which is ambiguous in some cases, fuzzy-based approach is a prospective solution. Fuzzy logic provides the ability to use data values that can have a specific range of values that are resolved at runtime; offering flexible, adaptive and extensive abilities for the system. Furthermore, the strength of fuzzy logic is that it can represent a vague term, such as “low" or “high", “bad”, “acceptable” or “good”, which obviates the need to choose a specific value. Also, fuzzy parameters can be optimized using machine learning or bio-inspired techniques. Due to these benefits, fuzzy logic is widely used for various applications including digital image processing, elevator control, and pattern recognition.

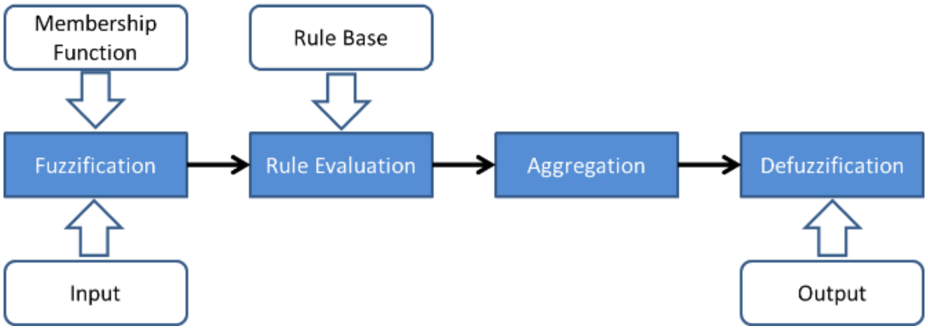
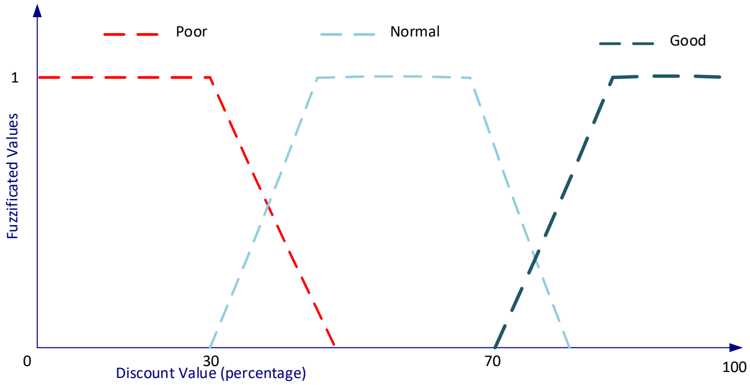


Figure 7-3. Mamdany Fuzzy Interference System procedures

To this purpose, the fuzzy approach is used for the Human-to-Vehicle knowledge extraction. The ambiguous TAs parameters are easily represented (both by range of values or linguistic values where vagueness is associated). We take an example to demonstrate the evaluation of *Pricing*, a TA of *Human-to-vehicle* Knowledge, using Mamdani FIS. The TA *Pricing* comprises of two properties *Discount* and *Fuel Consuming* which are translated into fuzzy sets using the associated membership functions in the Fuzzification process (Figure 7-4). For example, if the *Discount*, which is 25%, is entered as an input, then the associated membership function then evaluates and maps the input to a value in the fuzzy set, in this case “poor”, instead of “normal” or “good”. If the *Fuel Consumption* is 45 Miles per Gallon (MPG), the associated membership function maps the input factor to “low”, instead of “medium”, “high”, or “extremely high”.

The evaluated results are then passed to the Rule evaluation step. In this step, membership values, which were passed from the Fuzzification step, are evaluated using fuzzy rules stored in the Rule base.



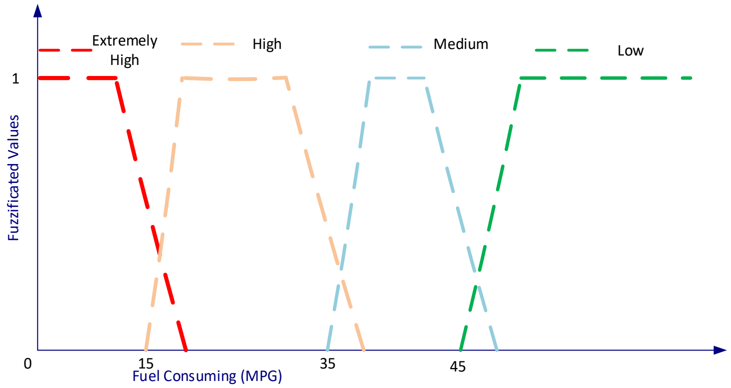


Figure 7-4. Membership functions for Discount and Fuel Consuming

The Mamdani scheme is a type of fuzzy relational model where each rule is represented by an If–Then Relationship. Output of the Mamdani fuzzy model is represented by a fuzzy set. In order to normalize the Knowledge TI, the outputs, in the form of fuzzy values, need to be converted into crisp values, which is the final process of the system called Defuzzification. One of the most popular defuzzification methods is the Centre-of-Gravity (CoG) method. Equations (7-1) and (7-2) are CoG based defuzzification formulae in continuous and discrete form respectively.

$$COG(A) = \frac{\int_x \mu_A(x).x.dx\text{-}}{\int_x \mu_A(x).dx} \tag{7-1}$$

$$COG(A) = \frac{\sum_{q=1}^{Nq} \mu_A(x).x}{\sum_{q=1}^{Nq} \mu_A(x)} \tag{7-2}$$

Note that membership functions and fuzzy rules could be automatically raised by a reasoning mechanism based on a machine learning technique with information model from an ontological model of entities in IoT. For simplicity, in the car-sharing example, these functions and rules are pre-defined.

7.2.2. Trust Evaluation using Utility Theory

We propose a Utility Theory mechanism for a personalized overall trust value. Trust evaluation is a dynamic process which heavily depends on a trustor's preferences. Each trustor needs both appropriate trust data and aggregation methods for producing desired information which reflects the trustor perspective. Specific trustors might use and define different trust computation methodologies for dealing with their associated trust data. For example, in our proposed trust infrastructure, the weights for TIs (Recommendation, Reputation, and Knowledge) reflect the trustor’s preferences, resulting in the calculation of overall trust value. The trustor could assign weight for Knowledge as highest since he/she is expertise in vehicle rental, the other could choose the highest weight for both Recommendation and Reputation because he/she believes in opinions from others. We denote the entity profile as the triple tuple *UP* ($W_{recommendation}$, $W_{reputation}$, $W_{knowledge}$).

In this trust calculation module, we define a utility function to calculate the overall trust by applying a weighted *UP*. An additive aggregate utility function is used [190] which aggregates multiple criteria in a composite criterion, using the information given by a subjective ranking. The *UP* then is used as a subjective ranking:

$$\textit{Trust Score} = \textit{vector } UP(W_{recommendation}, W_{reputation}, W_{knowledge}) \ x \ \textit{vector } TI(\text{Recommendation, Reputation, Knowledge})$$

UP could be predefined for basic users or manually chosen for advanced users who understand the complex trust system. For a better profiling mechanism, our system should take these challenges into account:

- Profiling process is typically either behaviour-based or knowledge-based. The former creates static models of entities and dynamically match the entities to the closest model whereas the latter uses the entities' behaviour as a model, typically using machine learning techniques to discover useful patterns in the behaviour.
- Knowledge must be acquired in order to create the entity profile. The model is then refined by monitoring subsequent behaviour.
- Entity profile should be organized by the system using some mechanisms in order to easily find similar items.

7.3 Knowledge-based Trust Evaluation using Inference Engine in Data Exchange and Sharing

Our previous studies have proposed a conceptual model based on Usage Control (UCON) and a handling mechanism for data access control in Smart City in which stakeholders can put their preferences in the form of constraints and obligations on the use of data [191, 192]. However, the proposed model cannot cope with many complex scenarios. For example, a commercial company requests all details of energy usage data on an hourly basis, but the stakeholder sets a policy in which only institutional actors are permitted to access data in detail whereas commercial operators are permitted only statistical data on a weekly basis. The reason is the data owner "thinks" that institutional operators are securer than commercial actors. We believe that stakeholders only share data if they "trust" the participants regardless of the type of actors. The success of any data sharing platform depends on the compliance with data protection regulations and, beyond legal obligations, with trust relationships between stakeholders and data consumers.

Our solution is to integrate a trust service platform to a UCON mechanism called Trust-based Usage Control (TUCON) that can guarantee data is only permitted to be accessed and obligated by trusted sources. TUCON offers several benefits such as policy enforcement based on attributes of stakeholders and consumers, based on obligation actions, and based on trust. It offers data abstraction and data monetization features, and offers on-the-go usage decision control that adapt with environment changes. The main contributions in this paper are the following: (i) a novel trust service platform with a trust model, a system architecture, and a trust computation procedure. (ii) TUCON: a novel usage control conceptual model and architecture for Smart City that considers three basic UCON factors: authorizations, obligations and conditions regarding the trust platform. (iii) We provide formalization and prototype for both trust service platform and UCON including data abstraction, data annotation, semantic and reasoning mechanism.

7.3.1. Background and Related Work on Usage Control

UCON is a new model of access control and was initially proposed by Sandhu and Park [193] with a purpose of addressing emerging digital environments, allowing application in various access control situations. UCON enables two advanced features to cope with a dynamic networking environment: (i) mutability of attributes, and (ii) continuity of an access decision. Basically, UCON keeps track of changes of attributes and policies when access is in progress, resulting in being able to change permission decisions. Then an authorization system revokes granted rights or terminates resource usages accordingly. The permission decision is determined based on three factors called Authorizations, Obligations and Conditions. Authorizations are predicates over subjects (data consumers) and/or objects (stakeholders, data) attributes and put constraints on them to judge and grant the subjects a certain right on the objects. Obligations is a novel component in the UCON model that examines the accomplishment of compulsory tasks that subjects have done to objects before, during and after access period. Conditions are constraints from environment attributes, not related to both subjects and objects but affecting the usage decision process[194]. A notable advantage of UCON is the expressiveness of policies and obligations applied in various access scenarios. UCON not only conveys capability of existing access control models but also goes beyond them.

There is much research literature working on UCON for data sharing in some emerging network environments such as Social Network, Cloud Computing, the IoT and Smart Cities. UCON features and research challenges have been well studied in a survey conducted by A. Lazouski and his colleagues in [195]. Authors in [194] have extended traditional access control models for providing obligations and conditions when accessing enterprise resources, forming a simple usage control mechanism. A simple accountability model and a platform has been proposed in [196] allowing participants to explore consequences of different usage control policies. A privacy model is proposed in [197] in which semantic web technologies are utilized for supplying a privacy model and offering users to impose their preferences and control over data in the Smart Grid environment. We have continued previous studies on data usage control [191, 192] by integrating with our trust platform introduced in [135]. We believe TUCON will open some approaches for a trust-based usage control model in IoT ecosystems.

7.3.2. Trust-based Usage Control Mechanism

TUCON Conceptual Model

The initial step in the design of any UCON mechanism is to identify objects to be protected, subjects that request to access and perform actions on objects. Actions are obligations describing how the objects are exploited by the subjects. It is necessary to define Access rights associated with each of the obligations and Authorizations that predicate the access rights based on attributes (ATT(O)), subjects attributes (ATT(S)) and the environment attributes as Conditions. In TUCON, objects are a dataset owned by stakeholders, subjects are data consumers, conditions are trust relationships between data owners and data consumers as illustrated in Figure 7-5. Details of the conceptual model is clearly described in the next sections.

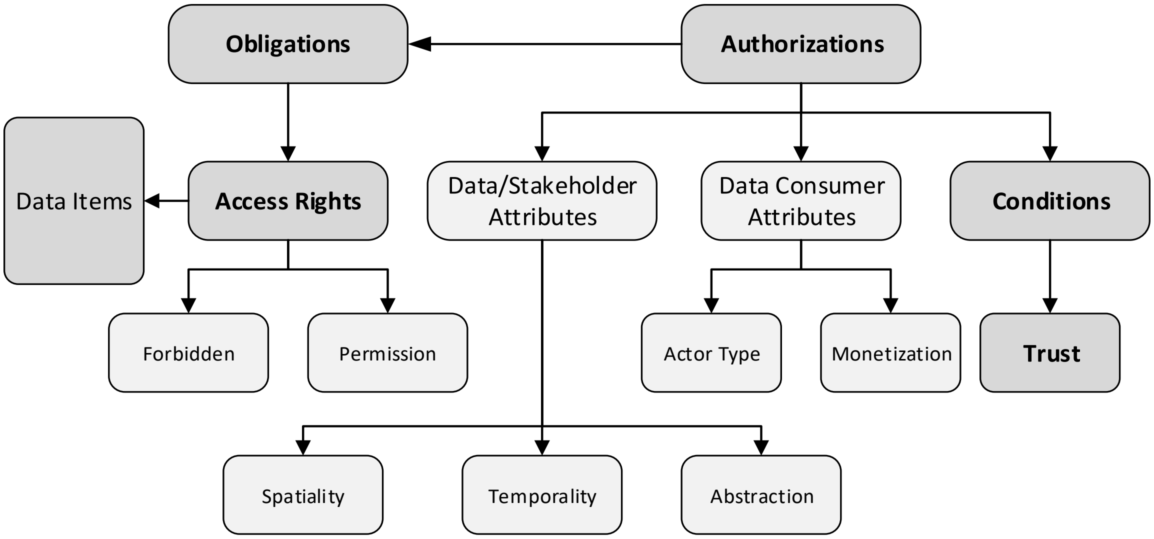


Figure 7-5. TUCON conceptual model

TUCON System Architecture

TUCON architecture is built under context of the 3-layered Smart City shared platform proposed in [198, 199]. The three layers are Infrastructure Layer (INF), Platform Layer (PLA) and Application Layer (APP). The platform is to deal with data acquisition and data annotation from deployed sensors exploited by multiple applications and services. The Data Manager (DM) is to work with IoT data and resources from INF whereas the Application Manager (AM) is an interface between application and PLA. An Ontology Manager (OM) is also introduced for data annotations and for supporting semantic-based

Wireless Sensor Networks (WSN) services using domain ontologies such as Semantic Sensor Networks [200].

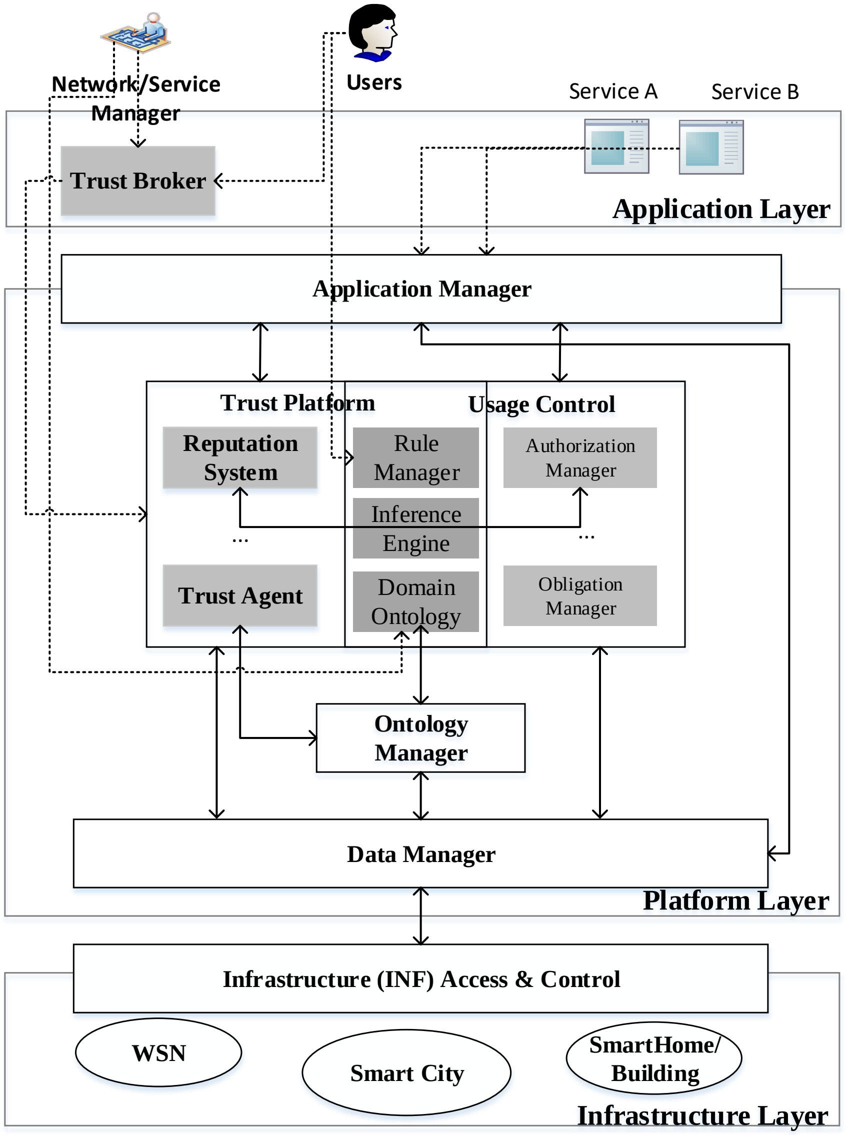


Figure 7-6. The proposed TUCON Architecture in the Smart City shared platform

The TUCON architecture is created by incorporating the TAMP and usage control components into the 3-layered shared platform. As illustrated in Figure 7-6, three mutual components are shared between TAMP and TUCON: Rule Manager (RM), Inference Engine (IE) and Domain Ontology (DO).

- RM is for handling rules in the trust knowledge base in TAMP and authorization policies (rules) in TUCON. Note that the rules express the relationships among classes and individuals of the ontologies, thus, incurring interactions among RM, DO and OM. RM directly interacts with Users for acquiring user preferences in the form of rules in the case of TUCON. RM also interacts with Trust Brokers for the user preferences in the case of TAMP.

- IE implements some reasoners for inferring new facts and trustworthiness in TAMP as well as inferring access rights for TUCON. TAMP can use same or different reasoners depending on their formalization types. In this study, we use Description Logics with Ontology for trust and Defeasible Logics (DLs) for usage control formalizations, resulting in different reasoning mechanisms being used.
- DO is a manager for handling domain-specific ontologies, and for cooperating with OM for data annotation and data abstraction in both TAMP and TUCON. DO directly works with Network/Service Manager for ontology update.

7.3.3. Practical Expression and Prototype

Elements and formalization of the TUCON conceptual model are depicted by implementing a prototype based on some semantic-web technologies and DLs. Details of the practical expression and prototype of DataItems, Data usage policies and Expression are described in APPENDIX A: 4.

TUCON Formalization and Expression

The approach for TUCON formalization is based on DLs, a non-monotonic formalism with normative conflicts-solving ability and low computational complexity [201]. Particularly, an extension of DL formalism enriched with model and deontic operators is used as a formal model for TUCON policies due to its representational capability of Obligations and Authorization factors [202, 203]. We take several examples to show how DL is applied for TUCON formalization:

- **Facts:** Facts in DL represent the ATT(O), ATT(S) and Condition (in terms of trust level). For example, two institutional organizations (IO1 and IO2) with "High" and "Low" trust value ,respectively, are represented as below:

```
F1TUCON(IO1): {ActorScope(Institutional)}

F2TUCON(IO1): {TrustScope(High)}

F1TUCON(IO2): {ActorScope(Institutional)}

F2TUCON(IO2): {TrustScope(Low)}
```

- **Rules and Superiority Relations:** All constraints among stakeholders, data, actors, conditions and TUCON AccessRight are represented in DL rules. Note that in DL, there are three different rule types which have different meanings. The strict rules can never be defeated, while defeasible rules can be defeated by contrary evidences. Strict rules and defeasible rules are used for drawing conclusions whereas defeater rules are only used to prevent from making conclusions. Superiority relations of rules are used to set the priority among these rules. The following is an example of defeasible rules and superiority relations of the two institutional actors IO1 and IO2:

```
R1TUCON(IO): {X[OB] => SpatialScope(Street)}

R2TUCON(IO1): {IO1[OB] => SpatialScope(any)}

R5TUCON(IO2): {IO2[OB] => SpatialScope(Zone)}


R2TUCON(IO2) > R1TUCON(X)

R3TUCON(IO2) > R1TUCON(X)
```

X represents any institutional actor. OB, short for Obligations action, is a modal operator of DL extension. The example can be explained as follows: by default, any institutional organization is allowed to conduct OB on data at spatial street level. However, this policy can be overruled when considering the trust relationship between the actor and the data owner. For example, if the trust value is high, then the actor can access all spatial levels of data (actor IO1) or if trust value is low, then only zone level of data is permitted.

- **DL Inference Engine and TUCON request:** An example of a consumer X requests for data with Obligation action OB will be expressed in DL as follows:

```
Rreq.TUCON(X[OB]):{SpatialScope(Street), TemporalScope(daily), AbstractScope(detail)
=>X[OB]}
```

A DL inference engine is used to get the conclusion that whether RreqTUCON is defeasible is proven in the DL theory or not. The inference algorithm is based on DL Proof Theory mentioned in [201]. Several candidates of DL reasoners can be applied and we choose Spindle[11] for our demonstration. The conclusion is as follows:

```
# Conclusions

===================

-D Rreq.TUCON(X[OB])

-d Rreq.TUCON(X[OB])

…
```

meaning that the Rreq.TUCON(X[OB]) request is Defeasible Provable in the DL theory. That means at this moment, the data consumer satisfies all the authorization policies to obligate the action OB on the stakeholder's data, the AccessRight now is Permission. The characteristic of the DL's formalism is suitable for any usage control mechanism since the facts, the rules are defeasible and

[11] http://spin.nicta.org.au/spindle/

can be overruled by supplying more facts, rules, and superior relations in DLs, resulting in conclusion changes. This feature enables the ability of continuity of an access decision in TUCON.

7.4 Experience and Reputation-based Trust Evaluation in Blockchain-based Systems

7.4.1. Introduction

The turn of the last century brought us to the Internet of Things (IoT) where billions of devices are interconnected. These devices range from simple RFID tags, sensing and actuating devices to complex systems like smartphones and smart vehicles producing massive amounts of data every second. It is expected that just two years from now (the year 2020) there will be more than 50 billion connected devices, approximately 6.58 devices per person on our planet [204]. There will be approximately 5,200 GB of data for every person on Earth, and the size of the 'Digital Universe' will reach to 44ZB (i.e., 44 trillion GB)[12]. The increasing number and connectivity of devices also results in dramatically increasing the flow of data exchange. The current Internet infrastructure enables us to send general information such as photos, text, audio and video files from your local computer to others at reasonable speed. How about in the future? Imagine that you are living in a smart home equipped with a variety of sensors and personal gadgets producing a vast amount of data every day. Your data will not be stored at your local devices but in the cloud. It is also predicted that data will be valuable goods in the era of the IoT, thus you can sell your data to others – this action is called 'data transaction'.

The question is: will data transactions operate in the same manner as we are currently exchanging information in the Internet? We think that it will not be. The first reason is that it is not suitable for exchanging vast amounts of data across the network which imposes extremely high overheads and can lead to dreadful operations upon the IoT infrastructure. This issue can be overcome by interchanging the ownerships, but not the data itself; then counterparts just need to access the data cloud storage for getting the data. Here, the ownerships are digitalized representing data, as one of the personal assets. In this sense, various types of assets such as a software program you develop, a song you compose, a picture you have, and even your real-estate you own can be transacted in the same manner – exchanging the represented value [205]. The second reason is that the current data exchange model is facing a problem called 'double spend'. That is when a person sends her information to others, she is not actually sending the information, but she is sending a copy of that. Therefore, the data can be sold many times. The 'double spend' problem can be got around by using

[12] https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm

a trustworthy (and powerful) intermediary for controlling the transaction [206]. The intermediary guarantees that the value will be securely and safely transferred and settled. However, as a coin has two sides, the involvement of such third-parties in value exchanges imposes delay in processing, single-point failure, introduce dread threats and risk, and importantly, comes at a cost. Fortunately, that is what Blockchain technology naturally deals with [207]. Blockchain technology is expected to have a huge impact on how people exchange their assets (both physical and digital ones) by enabling peer-to-peer (P2P) transactions of value in a secure manner. From the two above concerns, the novel paradigm “Internet of Value” (IoV) is coined. Generally, the IoV is the future expression of the Internet where everything can be symbolized or represented as digital values that are able to be directly and securely exchanged using Blockchain. Recently, several speeches from industrial companies such as TED[13] and Ripple Labs[14] have mentioned the term IoV and its provisions. To the best of our knowledge, this paper is the first academic article dedicated to developing IoV technologies.

In the IoV, Blockchain is expected to be used for value transactions resulting in security, integrity, and non-repudiation being assured. However, as Blockchain is immutable, that is when a transaction is verified, it is almost impossible to reverse. That means the peers you are dealing with should be trustworthy; and the terms and conditions in the transactions when exchanging value should not be exploited for cheating. Therefore, there should be a mechanism to evaluate trustworthiness of the counterparts that an entity is going to deal with; also to support the participants for negotiating terms and conditions for in the transaction. As a result, a trust platform is critical for strengthening and empowering the IoV. In this section, we briefly introduce the concept of the IoV and its conceptual system model; and focus more on developing a trust platform for the IoV leveraging the trust model called REK introduced in [100]. That is the two Trust Indicators (TIs) called Experience and Reputation will be calculated based on interactions which indeed are transactions between entities in the IoV that are already recorded in Blockchain. Apparently, from the perspective of trust, after each interaction, a trustor is more aware of its counterpart (a trustee) in terms of how well the trustee has accomplished the transaction. And by using a feedback mechanism, which is also based on Blockchain technology, the awareness among these entities can be securely recorded and shared over all entities in the IoV (so-called the IoV network). Based on the entities’ awareness after each interaction, the Experience and the Reputation TIs can be obtained, consequently, the trust relationship between any two entities in IoV can be evaluated. Note that in IoV scenarios, entities and users are exactly the same and used interchangeably. The main contributions of this section are three-fold:

[13] https://www.ted.com/talks/rachel_botsman_the_currency_of_the_new_economy_is_trust
[14] https://ripple.com/insights/chris-larsen-on-the-internet-of-value/

- Introduce the concept and provision of the IoV considering Blockchain technology and Smart Contracts concepts.
- Propose a trust-based IoV model consisting of the system procedures and features, the reference system architecture and components.
- Propose a trust platform based on the Experience and Reputation concept that utilizes the REK trust model [100] for evaluating trust between entities in the IoV.

7.4.2. Internet of Value: Background, Concept and Provision

To understand the concept of IoV, we start at explaining (distributed) cryptocurrencies. A cryptocurrency is a digital asset as a means of exchange accepted by participants in a transaction. Cryptocurrencies are not necessarily issued by a public authority or a bank, instead, they use distributed digital cryptography protocols to securely manage the creation and the transactions of the currencies, hence the name [208]. In this regard, cryptocurrencies are digital representations of value. Bitcoin was the first cryptocurrency introduced in 2009 and remains the largest in terms of market capitalization. Besides, numerous cryptocurrencies have been created as blends of bitcoin alternatives. Bitcoin and its derivatives are deployed in a distributed manner using Blockchain database in the role of a distributed ledger. Such cryptocurrencies provide some key benefits that the traditional currency cannot. For example, verification and settlement of payment can be done in seconds (or minutes) regardless of geographical distance. There is no exchange rate, no intermediate fee, and just a low cost of transaction verification because transactions are done directly without the need for a third-party service provider [209]. The “double spend” problem is also completely eliminated by the Blockchain native characteristic through miner verification of proof-of-work (PoW) process [210].

Bitcoin and other crypto protocols are one of the most interesting cutting-edge developments in the payments industry, however, beyond that, the true enormous buzz is that transactions of various types of assets, not only the cryptocurrencies, could be manipulated based on the Blockchain technology. That is a Blockchain-based Value Exchange layer could be incorporated for asset exchanges such as “physical and digital properties, equities, bonds, AI, and an enormous wave of applications which have not yet been conceived” [211]. This is the initial idea of the IoV concept.

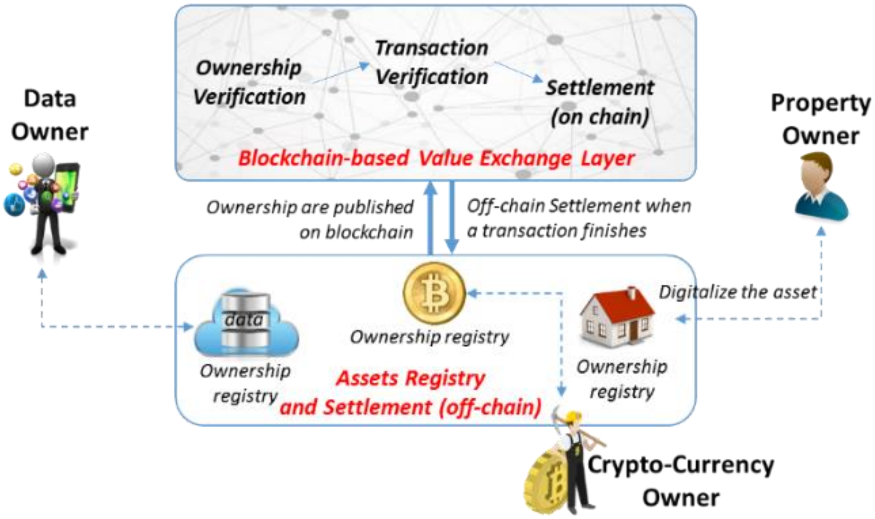


Figure 7-7. Concept of the IoV model in which assets are digitalized and exchanged on top of the Blockchain-based Value Exchange layer

As illustrated in Figure 7-7, the IoV conceptual model requires two main components to be built: (i) the Assets Registration and Settlement and (ii) the Blockchain-based Value Exchange layer. The first component (i) is business and management related that are out the scope of this paper. We mainly focus on developing the second component (ii) based on Blockchain and Smart Contracts that recently has attracted a large number of government institutions and private companies. It is provisioned to be an additional layer in the IoT for value exchanges (so-called Value Exchange layer). Blockchain provides mechanisms for securing transactions of value where Smart Contracts are agreements on value exchanges with terms and conditions between the participants in a transaction [212]. Smart Contracts are in the form of logics (computer code) and are accomplished and recorded on top of the Blockchain-based Value Exchange layer.

Blockchain and Value Exchange Layer: Background and Related Work

Blockchain is a distributed immutable database that consists of a continuous growing list of blocks. A block is a record of one or some transactions between peers in a network. Thus, two types of record can be found in a Blockchain: blocks and transactions. Transactions are encrypted using mathematical algorithms and need to verify (be signed) for validity before being hashed and encoded into a Merkle tree whose Merkle root is the hash of the considering block [213]. Each block contains a timestamp, a unique ID (i.e., the hash of the Merkle tree), and the ID of the prior block as the link between the two (Figure 7-8).

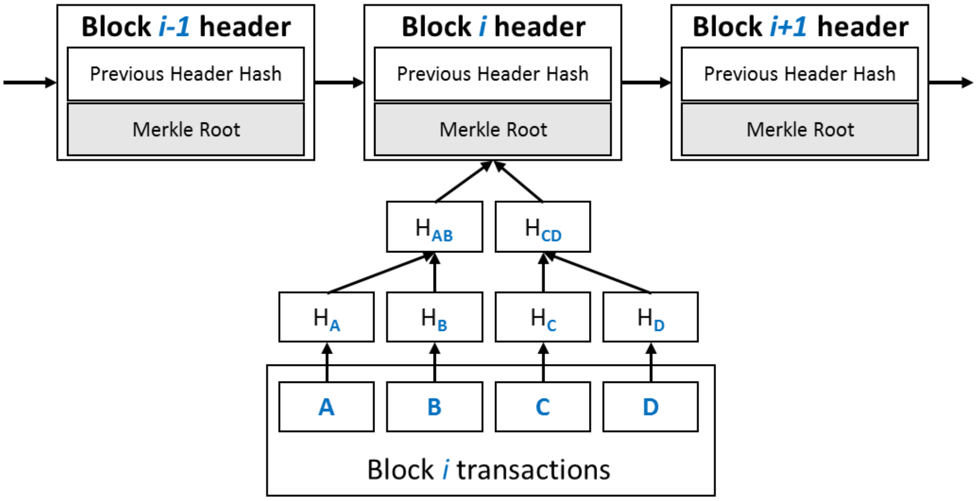


Figure 7-8. Blockchain, Blocks, Transactions and Merkle Tree

In Blockchain, a transaction is verified to be valid if and only if more than 50% nodes in the network reach consensus about its validity (the principle of Longest Chain Wins) [207]. In case of being valid, the transaction will be appended in the existing chain of blocks, synchronized and distributed across the network, thus, every node in the network has exactly the same copy of the database. This is why Blockchain is considered as an open, distributed ledger. By nature, Blockchain is inherently resistant to data modification. Once recorded, data in any given block cannot be altered retroactively as this would invalidate all hashes in the previous blocks in the Blockchain. The only way to modify a stored transaction in chain is to alter all subsequent blocks located in more than 50% of computers in the network, which is greatly challenging [214]. Consequently, Blockchain technology opens a new type of distributed ledger for recording transactions securely and efficiently. The ledger can also be programmed in order to verify, audit and trigger transactions in an inexpensive, consistent and automatic manner [215].

The Blockchain concept was introduced and implemented as a key component in the Bitcoin digital currency by Satoshi Nakamoto nearly a decade ago [207]. The use of Blockchain as a public and distributed ledger for Bitcoin transactions made it the first cryptocurrency not only to transact digital money in a secure and inexpensive way, but also to resolve the long-standing problem of "double spend" without the need for a trusted and powerful third-party. Since then, the Bitcoin design has been the inspiration for other cryptocurrencies. Interestingly, over the last two years, Blockchain has been provisioning to be a key technology to create a secure platform for directly exchanging not only digital money but also various kinds of assets including intellectual property, rights and wealth [216].

Smart Contracts

Smart Contracts are agreements between the participants of a transaction for exchanging assets [212]. In the IoV environment, Smart Contracts are decentralized arbitrary acts performed upon the Blockchain-based Value Exchange layer. This is different from traditional centralized arbitrary E-systems which are based on central contract systems. In the IoV, Smart Contracts are written on to Blockchain in which the participants involved are anonymous (only Blockchain ID (or address) shown) whereas the contents of Smart Contracts are public. As an agreement established by the parties involved, a Smart Contract consists of terms and conditions written under computer code and carried out on top of the Value Exchange layer [217]. The terms in a Smart Contract dictate movement of value based on conditions met. For example, the ownership of the data is changed from the data owner to the data buyer; in exchange, some amount of Bitcoin is transferred from the data buyer to the data owner. All of the steps for the event trigger, value movement and transaction settlement are achieved by Blockchain. The Assets Registry component sometimes plays in the settlement for off-chain assets (assets require further government administration when being exchanged) (Figure 7-7). An example of a Smart Contract can be found in APPENDIX A: 5.

The use of Blockchain is to create a distributed, immutable storage; whereas the use of Smart Contracts on top of the Value Exchange layer brings distributed, immutable escrows. This sets the IoV apart from other Blockchain-based applications.

7.4.3. Trust in the IoV Platform

Although Blockchain is the driving force behind the IoV that assures security, integrity, and non-repudiation of value transactions; beyond that, trust also plays a crucial role in empowering the IoV. The use of trust in the IoV is two-fold: (i) to help in evaluating assets; and (ii) to encourage transactions in the IoV by providing trust evaluation between participants for making contracts of transactions. This section proposes a conceptual trust-based system model with Blockchain for the IoV.

The REK model in the IoT environment is utilized for evaluating trust in the IoV. In the REK model, trust is comprised of the three indicators Reputation, Experience and Knowledge; however, in the IoV, there is not yet available information for quantifying the Knowledge. Instead, transactions between entities are recorded in Blockchain and distributed to peers in the IoV network, which is suitable for the Experience and Reputation calculations.

Conceptual Platform and Procedure for Trust-based IoV

The procedure for value exchanges for the trust-based IoV platform is described in Figure 7-9. The procedure consists of four major steps in an IoV transaction: (1), (2), (3), (4-1) and (4-2). The Smart

Contract establishment (1) and Trigger Events (2) are described in the Smart Contract section above. The steps (3) and (4-1) are the native functions of Blockchain technology. Two trust-related components called Trust Evaluation and Value Evaluation are also introduced in the platform. Although the latter component is out of scope, we still present an example about data evaluation to describe how trust is used in assets evaluation.

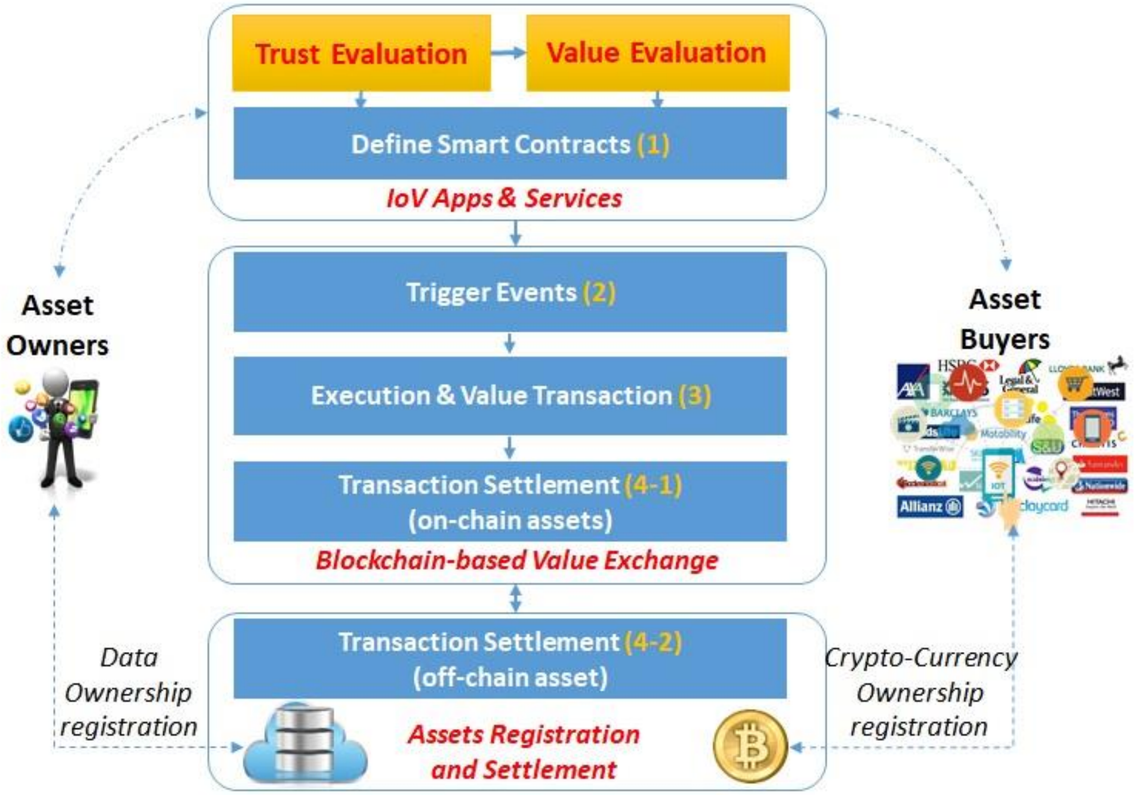

Trust Evaluation
Value Evaluation
Define Smart Contracts (1)
IoV Apps & Services
Asset Owners
Asset Buyers
Trigger Events (2)
Execution & Value Transaction (3)
Transaction Settlement (4-1) (on-chain assets)
Blockchain-based Value Exchange
Data Ownership registration
Transaction Settlement (4-2) (off-chain asset)
Crypto-Currency Ownership registration
Assets Registration and Settlement

Figure 7-9. Conceptual Platform and Procedure for Value Exchanges in Trust-based IoV

The main target is to evaluate trust between IoV entities to support transactions with trustworthy counterparts and also to negotiate terms and conditions when making Smart Contracts. That is, the users base decisions on trust to decide whether they should exchange assets with unknown counterparts without any trusted third-parties in IoV because once a transaction is settled, it is impossible to retract. This means that a user needs to have a clue of “belief” or “assurance” of its counterparts before making any decision to transact with. The below example illustrates how a Smart Contract can leverage trust as a trigger event to automatically withdraw risky transactions.

```
event Checking(address trustor, address trustee, float threshold);
function trust_checking(address trustor, address trustee, float threshold) {
    if (Trust_Evaluation[trustor, trustee] < threshold return;
    Transaction(trustor, trustee);
}
```

Also, terms and conditions in Smart Contracts should be decided based on value evaluation that an asset is more valuable if its owner is trustworthy and vice versa.

Reference Architecture Aligned with the IoT

The proposed IoV architecture is aligned with the ITU-T IoT and Smart Cities & Communities reference model[15]. The additional components namely Trust, Value Evaluation, Asset Registry, and Value Exchange layer are introduced and aligned with IoT components in the ITU-T reference architecture as illustrated in Figure 7-10.

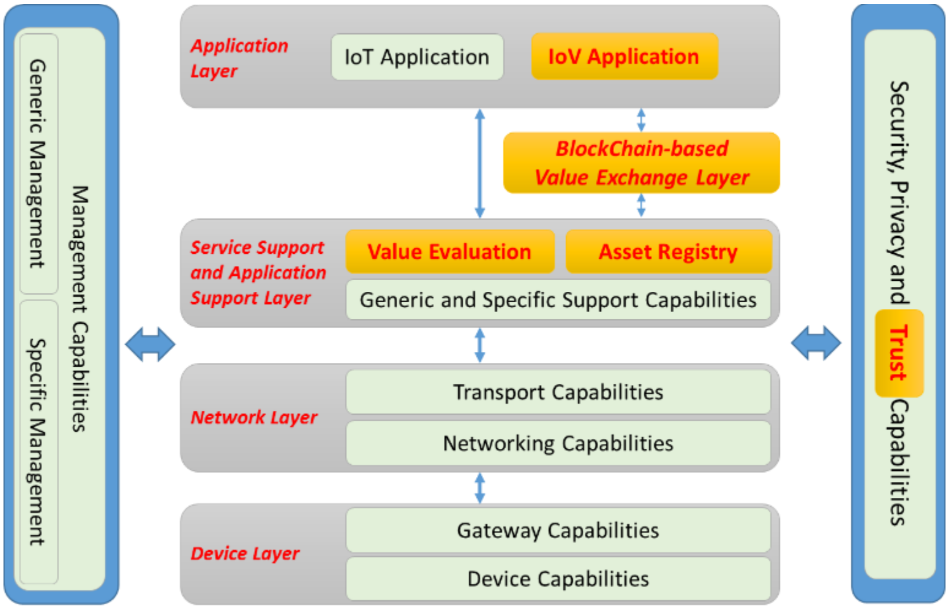


Figure 7-10. IoV High Level Architecture (HLA) Functional Model

As can be seen in Figure 7-10, the Value Exchange layer is located between the Application layer and Service Support and Application Support layer whereas Value Evaluation and Asset Registry components belong to Service Support and Application Support layer. The Trust component is same as Security and Privacy that is a multi-level capability interacting with all IoT layers from Device layer to Application layer.

Value Evaluation for IoV

Regarding the data transactions in IoV, as previously shown in the example of Smart Contracts, data can be exchanged with digital money. As a part of the Service and Application Support layer, the Value Evaluation component evaluates value for data to be exchanged and supports participants in establishing Smart Contracts in an automated manner. To do so, Value Evaluation mechanism takes three factors into

[15] http://www.itu.int/en/ITU-T/studygroups/2017-2020/20/Pages/default.aspx

account: trust value of the data owner, quality of the data, and forms of the data referring to the DIKW hierarchy[16] as illustrated in Figure 7-11.

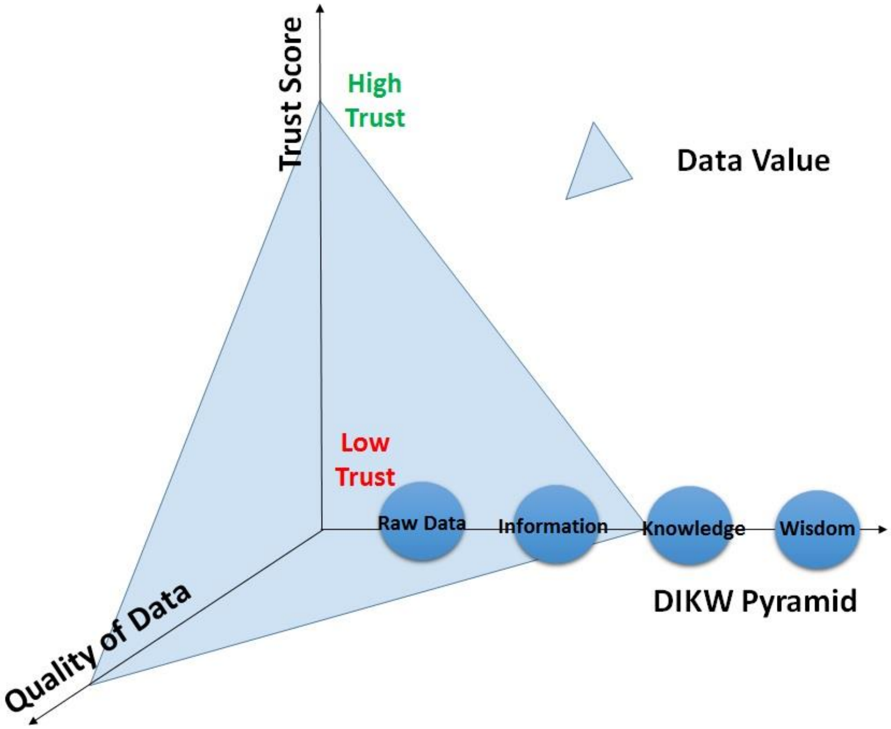


Figure 7-11. Data Value Evaluation based on three main factors: Trust of data owner, Quality of Data, and Data forms considering the DIKW pyramid

Normally, value of the data is high when the trust value of the owner is high, along with the high-quality data and the advanced form of data in the DIKW pyramid. This roughly demonstrates how data value is evaluated; and trust plays an important role in the evaluation scheme.

7.4.4. Trust Evaluation Platform in the IoV

To evaluate trust between entities in the IoV, we follow the trust definition in the IoT environment and the REK model proposed in [100]. We apply the REK evaluation model to IoV scenarios whose entities are anonymous and only entity ID (Blockchain address) and content of transactions are public. Thus, there is no available information for quantifying the Knowledge TI. Instead, all transactions with participants' IDs and timestamps are recorded and shared using Blockchain. And if a feedback mechanism is provided for sharing opinions of participants on these transactions, then the Experience and Reputation TIs are able to be calculated. In this section, we present a feedback mechanism for the trust platform along with the two computational models for Experience and Reputation TIs in order to evaluate trust.

[16] https://en.wikipedia.org/wiki/DIKW_pyramid

Feedback Mechanism

To establish and evaluate trust in the IoV, a feedback mechanism needs to be deployed for gathering information about participants who are involved in IoV transactions. Therefore, when any transaction is completed, the feedback mechanism enables participants to give opinions about how their counterparts have done to fulfil the terms and conditions in Smart Contracts. Feedback can be in both implicit and explicit types; and may or may not require human participation [181].

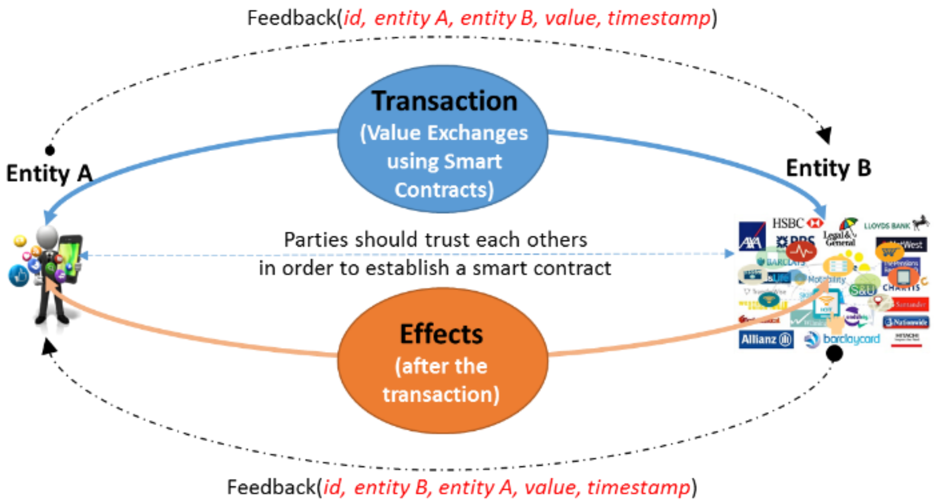

Feedback(id, entity A, entity B, value, timestamp)
Transaction
(Value Exchanges using Smart Contracts)
Entity A
Entity B
Parties should trust each others in order to establish a smart contract
Effects
(after the transaction)
Feedback(id, entity B, entity A, value, timestamp)

Figure 7-12. Feedback mechanism in Trust Platform for IoV transactions

As illustrated in Figure 7-12, the feedback mechanism enables entity A and entity B to share their opinions about the counterparts after exchanging their assets using Smart Contracts. The value of the feedback is personally evaluated based on how each entity perceives the effects after the transaction. The feedback mechanism also incorporates Blockchain technology to create a feedback blockchain along with the transaction blockchain. Each feedback consists of a source (i.e., Blockchain address of the entity (source entity ID) that gives feedback), a destination (i.e., Blockchain address of the target entity (target entity ID)), value of the feedback, and the timestamp at the time the transaction is verified. The Trust Platform will look for this information in the feedback Blockchain to evaluate Experience and Reputation for inferring the final trust value.

Experience TI Evaluation Model

Under the perspective of trust, experience is an original concept from social networks indicating to what extent an entity (as the trustor) trusts another entity (as the trustee). Experience is a type of asymmetric relationship between two entities obtained from previous interactions between the two. After each interaction, the awareness between the trustor and the trustee is supposed to get better, as a consequence, Experience more correctly indicates the relationship between the two as illustrated in Figure 7-13.

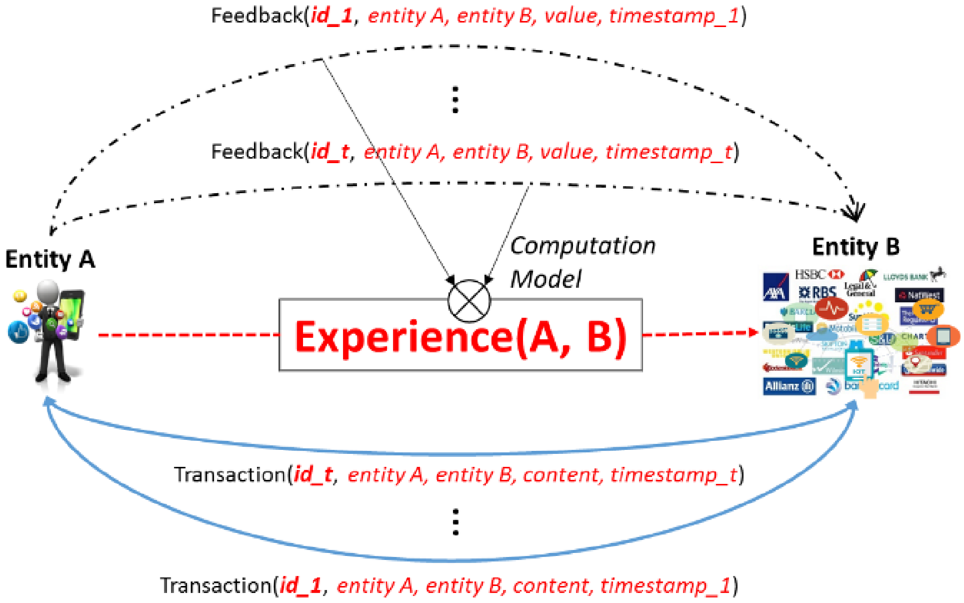

Feedback(id_1, entity A, entity B, value, timestamp_1)
Feedback(id_t, entity A, entity B, value, timestamp_t)
Computation Model
Entity A
Entity B
Experience(A, B)
Transaction(id_t, entity A, entity B, content, timestamp_t)
Transaction(id_1, entity A, entity B, content, timestamp_1)

Figure 7-13. Experience computation model based on feedbacks

To model experience relationships of entities in the IoV, we utilize the Experience and Reputation model and evaluation mechanisms proposed in CHAPTER 5.

Reputation TI Evaluation Model

Reputation (of an entity) is a concept that indicates the perception of a society about the trustworthiness of this entity. The goal of any reputation system is to provide an estimation of the entity's trustworthiness, thus, encouraging other entities to participate in transactions with the entity without first-hand knowledge. In the IoV with millions of users, only small number of users have already interacted with another, resulting in a very high possibility that two any entities are new to each other, thus no experience between the two. Therefore, reputation is the important information when evaluating trust. We also adopt the Reputation algorithm propsed CHAPTER 5 for quantifying Reputation of IoV entities. This reputation model is suitable to implement in the Trust Platform to calculate all reputation value for entities in a huge network like the IoV.

Finalize Trust Value

The final trust value is the aggregation of the two TIs: Reputation and Experience. a simple weighted sum for calculating final trust value between A (the trustor) and B (the trustee) in the IoV is as follows:

$$Trust(A,B) = \alpha Rep(B) + \beta Exp(A,B) \tag{7-9}$$

where $\alpha > 0$ and $\beta > 0$ are weighting factors that $\alpha + \beta = 1$. These weighting factors can be autonomously adjusted by breaking down and analysing feedback.

7.4.5. The Road Ahead

This section is a catalyst for IoV and trust-based IoV research that opens a variety of future work. The first direction is to investigate and develop IoV components such as Blockchain-based Value Exchange layer, the Asset Registry and the Smart Contracts. Related to trust, one direction can be a novel trust evaluation model considering more information about IoV entities than only feedback. Another direction is the adaptation of the Experience and Reputation models which requires to be adapted with parameters settings in a context-aware manner. The fourth direction could be a mechanism for a Value Evaluation component for a specific use-case that takes other factors, including trust, into account when judging asset value. We expect that our proposals can significantly contribute to further research activities in the future, taking into account Blockchain and trust issues for the IoV.

7.5 Trust Evaluation in Smart Parking Service in Smart Cities

In this section, a trust evaluation mechanism is integrated to a big system. In order to achieve semantic interoperability between many components including trust evaluation (called Trust Monitor component), agreement on common concepts is of key importance. This work is a part of the Wise-IoT project in which we have defined these key concepts for our use cases, re-using existing models where possible, e.g. based on FIWARE data models. In the following sections, the semantic models for the smart parking use-case is presented along with how Trust Evaluation mechanism is deployed and integrated. More information of this service can be found in APPENDIX A: 6.

7.5.1. Trust Evaluation Mechanism in Smart Parking Service

In the Wise-IoT project, trust is considered as the underlying psychological measurement of a service consumer (the trustor) indicating whether it should put itself into a risky situation in case a trustee turns out to be misplaced. To evaluate trust in the Wise-IoT platform called SAR, the model presented in the last section was used. Trust for the SAR scenarios are defined as “a belief of a trustor in a trustee that the trustee will accomplish the requirements as the trustor’s expectation”. For instance, in the Smart Parking use-case of the Wise-IoT project, trustors are drivers and trustees are parking spots where the drivers are going to park their cars. Thus, trust between a driver and a parking spot is the belief of the driver that the parking place will satisfy his/her requirements when parking there. The requirements could be the distance between the driver’s position and the parking space, could be the possibility of the parking place’s availability, or could be his personal preferences.

To establish and measure trust for the SAR, a feedback mechanism is a must for collecting trustors’ opinions on trustees whenever an interaction occurs. Therefore, when any transaction is completed, the feedback mechanism enables participants to give opinions about how their counterparts have done to fulfil the requirements of the trustors. Feedback can be in both implicit and explicit types; and may or may not require human participation.

The Trust Monitor aggregates the quality of information (QoI) from QoI monitor (component of the SAR as shown in Figure 56) and user feedback obtained to derive an evaluation for the trustworthiness. The processes above for the evaluation of TIs to establish and measure of trust depends on a feedback mechanism for collecting trustors' opinions on trustee whenever an interaction occurs. Therefore, when any transaction is completed, the feedback mechanism enables participants to give opinions about how their counterparts have done to fulfil the requirements of the trustors. This feedback mechanism can be either implicit or explicit; and may or may not require human participation. This feedback mechanism in the Wise-IoT platform enables users to share their opinions about an interaction after such an interaction is completed.

This section presents the necessity of QoI as an indicator of trust in a variety of IoT applications and services along with an evaluation model based on QoI and users' feedback.

QoI as an indicator of Trust

Various use-cases have been investigated in which trust is utilized for supporting users to select proper options in a recommendation system and deliver better quality of services (QoS). The need for trust in IoT applications and services can be clarified by taking the smart parking use-case in our ongoing Wise-IoT[17] project as an example. In this, parking services, an end-user requests an available parking lot close to a destination in a specific timeslot. Under the context of trust, the user requests finding a parking lot that she trusts to park her car. Therefore, the parking sensors show the availability of a parking lot; and traffic sensors to precisely infer the estimated time of arrival (ETA) from the user's position to the parking place should be working correctly. Here, the QoI scores are able to indicate the status of the parking sensors and the traffic sensors. However, only QoI scores might not be enough for illustrating the users' trust toward a parking lot. Other factors also contribute to how a user selects a parking lot including user's preferences, previous experience, or the reputation of the parking service. Such factors could be demonstrated and quantified by assembling users' experiences and opinions using a feedback mechanism. Nevertheless, as any IoT applications and services heavily depend upon collected data, QoI plays a crucial role in indicating and evaluating trust between users and IoT services.

Utilization of the REK Trust Model based on QoI and Feedback

[17] http://wise-iot.eu/en/home/

To establish and evaluate trust relationships between service requesters (i.e., trustors) and service providers (i.e., trustees), we leverage the REK conceptual trust model in the IoT environment proposed in [100, 168] which consists of the three major indicators as Reputation, Experience and Knowledge. The Knowledge indicator is "direct trust" inferred from attributes of a trustee whereas Experience and Reputation are "indirect trust" calculated from previous interactions illustrating personal opinion and global perspective toward the trustee, respectively. In this section, the REK model is utilized as illustrated in Figure 7-14. The Knowledge indicator is evaluated as QoI score; other trust-related attributes are neglected due to unavailability or not being suitable to collect; however, in some use-cases, other useful information could be gathered and plays as a supplemental factor in evaluating Knowledge. The other two indicators are calculated based on previous research works [100, 168] and briefly presented below.

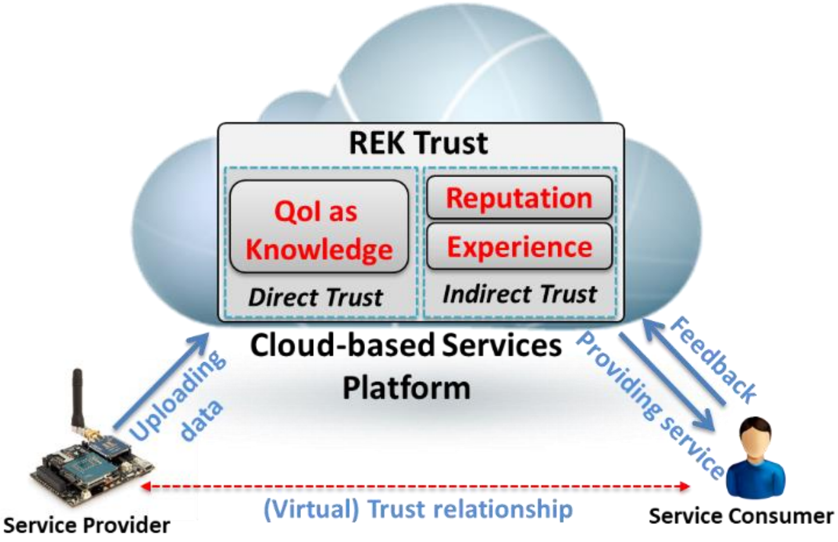


Figure 7-14. Utilization of the REK Trust Model based on QoI and Feedback in variety of IoT applications and services

User Feedback Mechanism and Implementation

The WISE-IoT version of the Supersede *jQuery* plugin handles all functionality related to user feedback forms: it communicates with the Adherence Monitor through the SAR façade to receive the feedback form templates, it displays a feedback form according to the templates, it checks user inputs for validity (e.g., it checks that mandatory questions are answered), and it sends the submitted feedback form to the SAR façade. The use of Feedback mechanism and the implementation can be found in APPENDIX A: 7.

Quality of Information Monitor Mechanism and Implementation

The QoI module classifies data quality problems and calculates QoI scores for the QoI dimensions: syntactic accuracy, semantic accuracy, completeness, uniqueness, and timeliness based on previously defined data quality rules. The information quality score metrics are based on the simple ratio calculation as described in [218]. The simple ratio is measured by subtracting the ratio between the total numbers of axioms that violate data quality rules for a dimension and the total number of axioms (DV), we proceed with the same manner for each dimension to generate a score for each dimension QoI_{dim} in (7-10). For the final score, we choose an "importance weight" approach[18], which is intended for programmers, not data analysts" to influence the final score w_{dim} (7-12). This weight can be attributed directly by the user or in the semantic description using Weighting Ontology[19] (*wo:weight*).

$$QoI_{dim} = 1 - (\frac{\text{DV}}{\text{T}}) \tag{7-10}$$

$$QoI = \sum_i w_i \times QoI_i \tag{7-11}$$

where *i* represents the dimensions. The QoI also supports the case where the user provides a weight for each property for more precision *wp* (7-12), the same as the first case, the user still can manually provide it or directly to the annotation (*wo:weight* as a subclass of the main *wo:weight*) according to the Weighting Ontology.

$$QoI = \sum_i w_{i,j} \times w_i \times QoI_i \tag{7-12}$$

where $w_{i,j}$ is the weight of property *j* of dimension *i*, and w_i is the weight of dimension *i*.

In the following sections, we explain the semantics and composition of each dimension based of the quality rules that provide the semantic validator. Table 7-1 shows the mapping of the quality inspectors, plug-ins that can be customised by the user, implemented in the ontology validator and the QoI dimensions:

TABLE 7-1. DQ DIMENSIONS WITH DQ RULES

DQ dimensions	DQ inspectors
Semantical Accuracy	The resonning capabilities [7]
Syntactical Accuracy	Literal Inspector: Checks literals for syntactically correct language codes, syntactically correct datatype URIs (using the same rules as the URIInspector), and conformance of the lexical form of typed literals to their datatype.
Completeness	ConsistentType Inspector: checks that every subject in the model can be given a type which is the intersection of the subclasses of all its "attached" types -- a "consistent type". For example, if the model contains three types Top, Left, and Right, with Left and Right both being subtypes of Top and with no other subclass statements, then some S with rdf:types Left and Right would generate this warning.

[18] https://www.stata.com/statalist/archive/2003-02/msg00525.html

[19] http://smiy.sourceforge.net/wo/spec/weightingontology.html

	VocabularyInspector: checks that every URI in the model with a namespace which is mentioned in some schema is one of the URIs declared for that namespace -- that is, it assumes that the schemas define a closed set of URIs.
Timeliness	Time Inspector: identify instances that represent an outdated state of the corresponding real world entity.
Uniqueness	PropertyInspector : checks that every predicate that appears in the model is declared in some -assumed schema or owl:imported model -- that is, is given rdf:type rdf:Property or some subclass of it. ClassInspector: Checks that every resource in the model that is used as a class, ie that appears as the object of an rdf:type, rdfs:domain, or rdfs:range statement, or as the subject or object of an rdfs:subClassOf statement, has been declared as a Class in the -assumed schemas or in the model under test.

Based on the previous section, the architecture of the QoI module is composed of two basic layers: i) the semantic validator web service that we have developed (see section II-C) and ii) a calculation module that takes the output of the first module and generates a score. The calculation module itself supports two different configurations. Figure 7-15 shows the case where the user directly provides the weights to the scoring module.

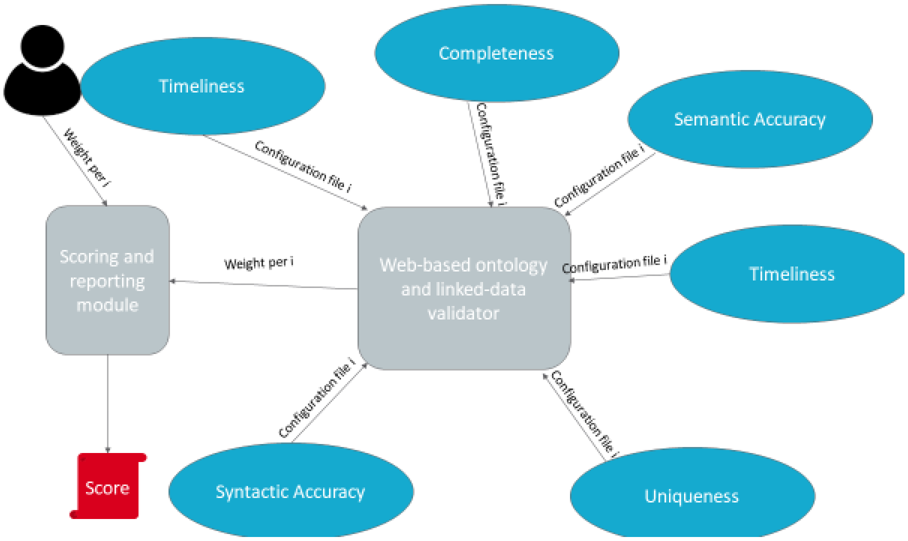


Figure 7-15: User as a weight provider

The second case is to provide the weighting factors within the annotations (*wo:weight*), for example, we can assign integer values ranging from one meaning "slightly important" to five meaning "task critical", the Weighting Ontology define a vocabulary for that purpose (*wo:max_weight* which is a decimal that describes the maximum, in our case the “important” task and *wo:min_weight* for the “less important”).

7.5.2. Trust Evaluation Deployment

This evaluation of trust supports decision-making of users. The trust framework was implemented and instantiated as a trust monitor as a cloud-based component, where all data collections, data pre-processing and trust evaluation mechanisms were deployed in a server providing interfaces for integration with other components. For example, the trust monitor has been integrated and deployed with the Self-Adaptive Recommendation system (SAR) where it interacts with quality of information component (QoI), traffic sensors and the Adherence Monitor (AM). The Trust Monitor functionality has been exposed as REST interfaces, with Trust Data store implemented locally using MongoDB as a standalone service. Detail of the deployment of the Trust Monitor module can be found here APPENDIX A: 8.

7.6 Chapter Summary

In this section, we have briefly introduced the proposed trust service platform that offers trust evaluation of any two entities to the IoT services for the Car sharing use-case. We modulate the human trust information process and social relationship to create a trust model by incorporating both reputation and knowledge-based. To deploy the trust service platform, all basic components and mechanisms are mentioned or described in detail in accordance with the trust car-sharing service. We have also introduced a novel usage control mechanism that leverages a trust platform called TUCON in order to provide more secure data access control based on a trust relationship between data owners and data consumers in Smart City environment.

A comprehensive concept, system model and architecture for the IoV with Blockchain and Smart Contracts for a secure and distributed value exchange network is also present. Beyond that, we have incorporated a trust platform for strengthening and empowering the trust-based IoV by utilizing the REK trust model. The trust evaluation system in the IoV leverages a Blockchain-based feedback mechanism for gathering opinions about entities involved in IoV transactions that are already recorded in Blockchain.

Finally, we introduce how to implement the REK model in the Smart Parking real-world service by investigating the data quality (i.e., QoI) and the relations with trust to evaluate trust between end-users and service providers and empower trustworthy IoT applications. We introduce a framework leveraging the trust monitoring system in relation to objective measurements of QoI data quality; as well as showing how QoI assessment and Trust evaluation are deployed in a real-world large-scale IoT environment. The validation of the framework is under investigation. A system called self-adaptive recommender (SAR) that has been developed and deployed in our testbeds for the Wise-IoT project will be used to verify and validate the work. The SAR system offers the dynamism needed to set up experiments and harvest data streaming needed for analysing the outcomes of the framework.

CHAPTER 8. CONCLUSION AND FUTURE WORK

8.1 Conclusion

In this thesis, I have provided a comprehensive understanding on the trust concept along with the REK model for evaluating trust by considering the three major TIs Reputation, Experience and Knowledge, respecting to the IoT scenarios. The proposed REK Trust Evaluation model with associated algorithms and mechanisms are then applied in various use-cases, showing the feasibility of adopting the model in the IoT environments and the feasibility of practical deployment in real-world applications and services.

In this thesis, the first objective on the augmentation of the generic trust concept, trust definition, and provide a conceptual model of trust in the IoT environment is successfully achieved by breaking down all possible attributes influencing trust. Here, the concept, characteristics, attributes, and model of trust not only in computer science but also in social science and psychology are investigated and analysed to come up with a comprehensive understanding of trust, influencing factors and TIs in the IoT.

The second objective is also achieved by the proposal of the REK trust model comprised of the triad, Reputation, Experience and Knowledge TIs. The REK model covers multi-dimensional aspects of trust by incorporating heterogeneous information from direct observation (i.e., Knowledge TI), experiences (i.e., Experience TI) to general opinions (i.e., Reputation TI). Variety of TAs are examined for covering the direct observation the Knowledge TI considering the three dimensions Ability, Benevolence and Integrity in various IoT scenarios. Knowledge TI is “direct trust” rendering trustor’s understanding on trustee in respective scenarios. Knowledge TI could be obtained based on limited available information about characteristics of the trustee, environment and the trustor’s perspective. Such TAs can be combined using some methods including Reasoning mechanisms and Fuzzy Logic for obtaining the evaluation of the Knowledge. I have also proposed mathematical models and calculation mechanisms for the Experience and Reputation TIs. Different aspects of the Experience and Reputation TIs are observed and based on that, associated mathematical models are carried out accordingly. Experience and Reputation TIs are originated from social features and extracted based on previous interactions among entities in IoT. Experience TI is an interrelation between a trustor and a trustee that reflects the personal perception of the trustor to the trustee. And by using a proposed aggregation model after each interaction, Experience TI can be obtained. Reputation TI, instead, is a property of the trustee itself which reflects the global perception about the trustee. Reputation could be calculated using a proposed graph analysis algorithm on the Experience topology utilizing Google PageRank algorithm. Finally, aggregation mechanisms are investigated for deriving trust from the associated TIs as the outcome of the REK evaluation model.

As the third objective, the REK Trust Model is utilized for a User Recruitment scheme in Mobile Crowd-Sensing (MCS) systems by considering interactions between MCS service requesters and data providers. Such interactions are established by leveraging the evaluation of quality of contributed data to MCS services with the Experience and Reputation models and mechanisms in the proposed REK trust model. The proposed REK Trust Model is also applied in a variety of other applications and scenarios such as Car Sharing service, Data Sharing and Exchange platform in Smart Cities and in Vehicular Networks using Fuzzy Logics and Reasoning and Inference Engine technologies; and also for strengthening Blockchain-based systems in the Internet of Value. The feasibility and effectiveness of the REK model and associated evaluation mechanisms are proved not only by the theoretical analysis but also by real-world applications deployed in our ongoing TII and Wise-IoT projects.

8.2 Future Work

I honestly believe that this research offers valuable understandings on trust as well as providing both generic and comprehensive trust models with prospective approaches and mechanisms for trust evaluation in the IoT environment. This PhD thesis could be a plentiful source and as a catalyst for others who are interested in doing research on trust, particularly in the IoT environment, and in real deployment of trust evaluation mechanisms. As a result, this thesis opens a large number of research directions in order to fulfil the trust evaluation platform as presented following:

- The first research direction is to adapt the trust evaluation model to various scenarios and use-cases in IoT context which requires to figure out a set of TAs for Knowledge TI in detail along with the adaptation of the proposed methods and techniques for evaluating the Knowledge TI. Also, appropriate parameters for the Experience and Reputation TIs mathematical model need to be autonomously adjusted reflecting the context-awareness of IoT scenarios. We are actively engaging in the adaptation of the proposed REK Trust Evaluation to Blockchain-based systems as a Blockchain framework is well matched with the evaluation mechanisms for Reputation and Experience in the REK model.
- The second direction regarding to Knowledge TI calculation such as an AI-based mechanism to obtain Knowledge TI from an unlimited available information throughout IoT ecosystems from physical, cyber and social worlds. Also a necessary mechanism needs to develop for reflecting the trustor’s propensity and environmental factors to the evaluation of Knowledge TI, such as an autonomous weighted sum with an AI module for adaptively adapting the weights of the TAs of the Knowledge TI in a context-aware manner.
- The third direction could be an AI-based rule generator for obtaining trust-related knowledge from variety of information in IoT ecosystems, which is then used as a trust knowledge-base for inferring

different TAs and Knowledge TI. In our demonstration on Knowledge TI calculation in previous chapters, the rules are predefined using understanding of the business models of particular use-case. And this can be improved by proposing a rule generator mentioned above using rule pattern recognition techniques.

- The forth direction is to improve the Reasoning mechanisms which is a prospective research work so that it can autonomously adapt with changes of the trust knowledge-base, resulting in an autonomous framework and with real-time data streaming (stream reasoning). The use of Semantic Web technologies such as the Ontology, RDFS and reasoning mechanism could be useful for more complex use-cases and for the support of real-time processing and scalability.
- The fifth direction could be other mathematical models for the Experience and Reputation TIs which are not only based on intensity and outcomes of interactions but also other complicated features extracted from particular contexts such as features of mutuality or difference in social environment. Also the future research work, respecting this direction, could be the adaptation of the Experience TI model and the Reputation TI model to a specific use-case which requires more investigation on appropriate parameters in the models.

APPENDIX A: PSEUDO-CODE, SNIPPETS AND EXPLANATION

1. Semantic Reasoning for Knowledge TI in the Cloud Web Hosting Service use-case

Cloud Web Hosting is a particular type of hosting platform service that allows organizations and individuals to put their resources in a cloud platform (a virtual server) instead of a physical web server. Cloud Hosting offers a powerful, scalable and reliable hosting service compared to traditional alternatives by leveraging the benefits of cloud computing [219]. For example, due to the decentralized and clustered cloud hosting system, the service is reliable in case of hardware breakdown, power disruption and natural disasters. However, the lack of centralization could give users less control on where their data is located, imposing security and privacy threats.

A question raised here is how to evaluate whether a Cloud Web Hosting service is good in terms of providing a trustful service. According to some discussions and surveys on the Internet, customers usually take the following features into account when purchasing a hosting service for their website:

- Reliability including uptime and downtime, monitoring and backup schemes
- Security including hardware and software firewall, geography, security mechanisms used in data centre
- Operating Systems, database and storage options
- Quality of Service including scalability and flexibility, responsive load balancing, delay and jitter
- Cost Effectiveness including price, service and maintenance supports

The priority and the level of importance of the above features when making a decision to purchase depend on each customer. This reflects the subjective characteristic of trust. We consider these features, classify and then modulate them as concepts in the trust ontologies.

Trust Lower Ontology for Cloud Web Hosting Service: The trust lower ontology is for describing the general concepts in the upper ontology in detail. It is also called domain-specific ontology. The creation of lower ontology requires several techniques in knowledge engineering such as knowledge acquisition for grasping sufficient TAs in the ontology [118]. The procedure to investigate domain-specific knowledge varies from interviewing with domain experts to data mining in networking resources as mentioned in the part C above. For example, in Cloud Web Hosting service, the Physical is constituted of Quality of Transmission and Quality of Device TAs. Each TA is also constituted of several technical specifications that are illustrated in Figure Appendix A-0-1. Similarly, the Cyber sub-TI for Cloud Hosting service is constituted of Quality of Information (QoI) and Quality of Service (QoS) TAs, each of them is formed from some networking features Figure Appendix A-0-2. The knowledge acquisition techniques also occurr in the creation of rules which is mentioned in the later sections.

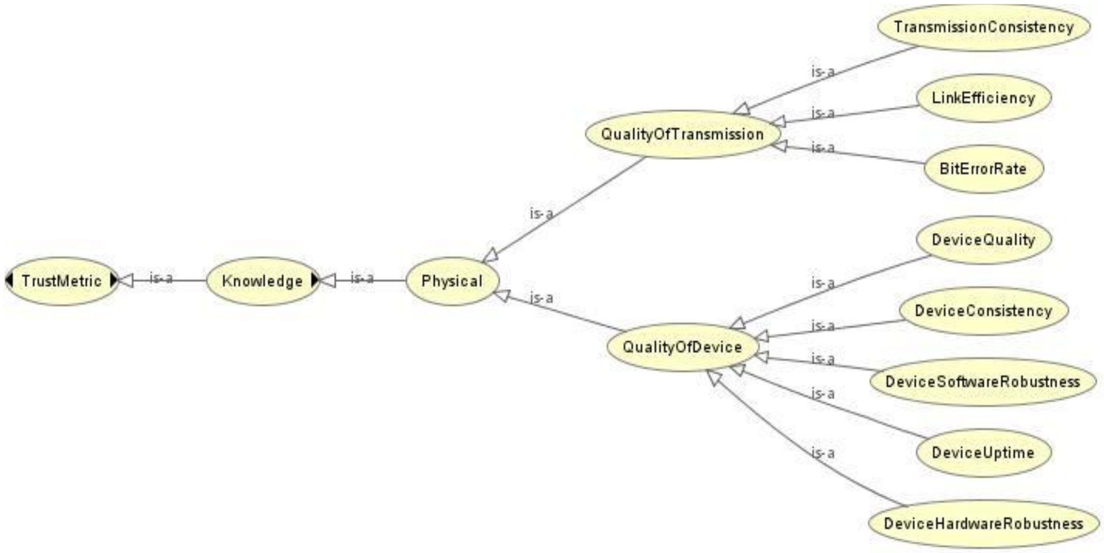


Figure Appendix A-0-1. Physical sub-TI in Lower Ontology for Cloud Web Hosting service

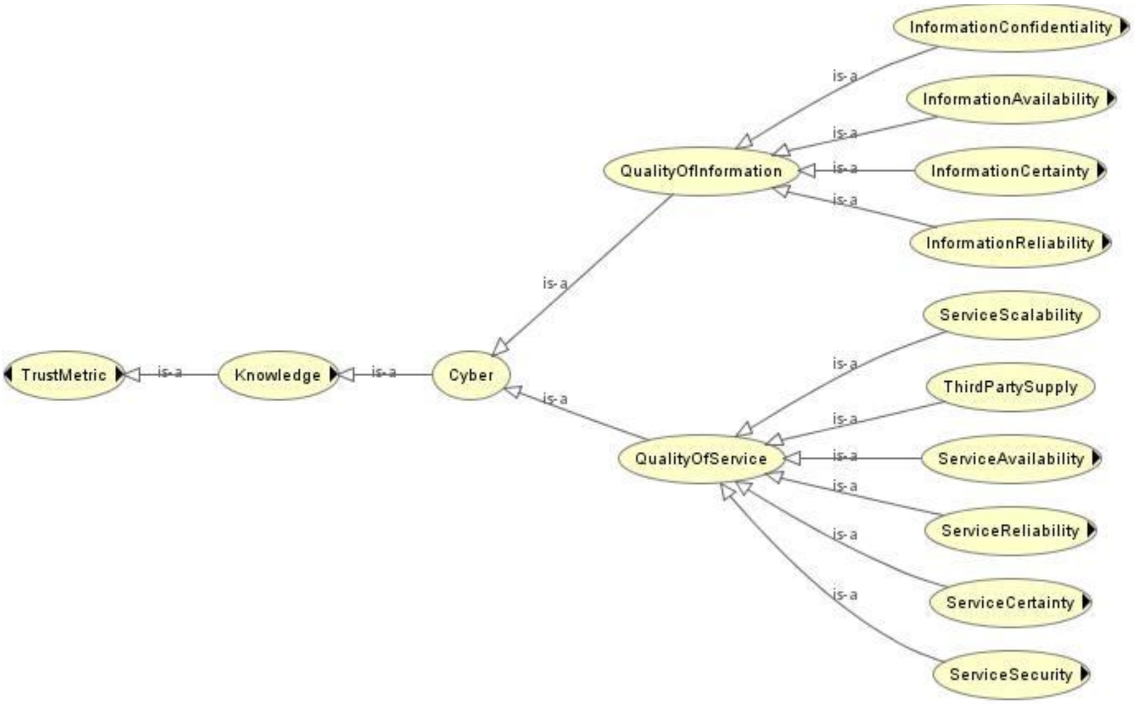


Figure Appendix A-0-2. Cyber sub-TI in Lower Ontology for Cloud Web Hosting service

2. MCS User Categories based on QoD Distribution

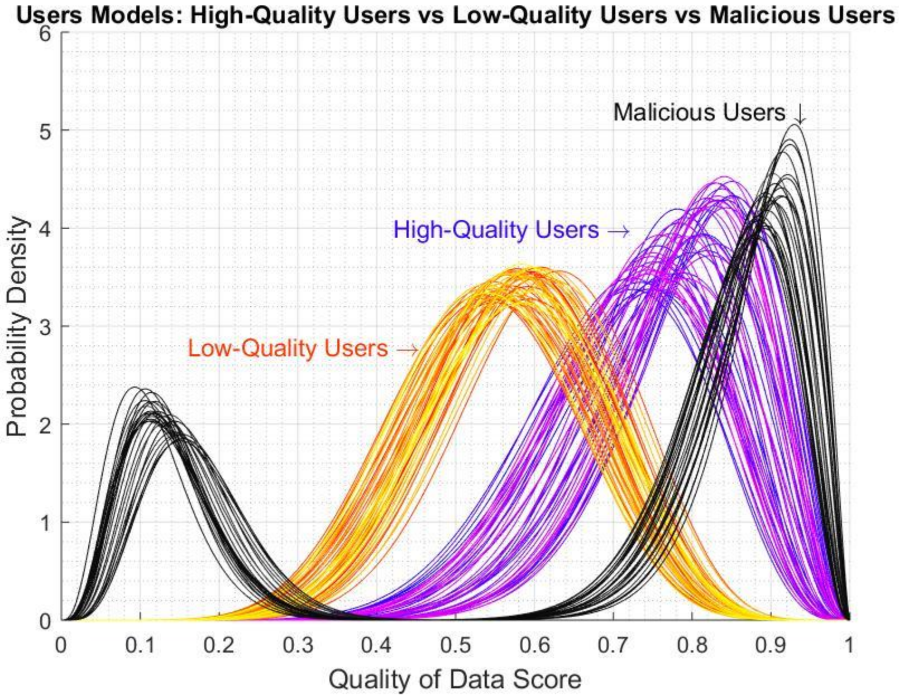


Figure Appendix A-0-3. User Models in MCS systems

- **High-quality Users:**

  High quality users are supposed to consistently produce high QoD in most sensing tasks. Based on the statistical information, QoD scores from a high-quality user are distributed in the interval (0, 1) but the highest distribution is in the range (0.75 – 0.85). QoD scores from a high-quality user follow a unimodal Beta distribution with two positive shape parameters $Beta(\alpha_{high}\, \beta_{high})$ satisfying $10 < \alpha_{high} < 15$ and $3 < \beta_{high} < 5$. The probability density function (PDF) of the Beta distributions for 50 high-quality users are shown in Figure Appendix A-0-3.

- **Low-quality Users:**

  Low-quality users consistently produce average or below-average QoD scores in most of sensing tasks. QoD scores are in (0, 1) interval but mostly fall in the range (0.5 – 0.65). Similar to the high-quality users, QoD scores from a low-quality user follow a unimodal Beta distribution with the two positive shape parameters $Beta(\alpha_{low}, \beta_{low})$ satisfying $9 < \alpha_{low} < 12$ and $7 < \beta_{low} < 9$. PDF of the Beta distribution for 50 quality users are depicted in Figure Appendix A-0-3.

- **Intelligent Malicious Users:**

  Even though there is no data which has been collected from malicious smart devices, we expect a feasible intelligent malicious user tends to follow the following behaviours:

- Normally produces very high QoD scores as the recruitment fishing purpose in order to be a strong candidate for recruitment schemes.
- Unpredictably and intentionally produces very low-quality data once the user is recruited in a sensing task to destroy a targeted MCS service. The service will be heavily damaged if the data is used for fulfilling requested services.

According to the above description, the malicious user model follows a bi-modal Beta distribution. Thus, firstly we define two Beta distribution models, one for very high QoD scores $Beta(\alpha_{mhigh}, \beta_{mhigh})$ satisfying $18 < \alpha_{mhigh} < 22$ and $2.5 < \beta_{mhigh} < 3.5$; and one for very low QoD scores $Beta(\alpha_{mlow}, \beta_{mlow})$ satisfying $4 < \alpha_{mlow} < 6$ and $25 < \beta_{mlow} < 35$. Then the two Beta distributions are mixed in order to form the desired bimodal Beta distribution $BiBeta$ using a mixture coefficient parameter γ as the follows:

$$PDF(BiBeta) = \gamma * PDF\left(Beta(\alpha_{mhigh}, \beta_{mhigh})\right) + (1-\gamma) * PDF(Beta(\alpha_{mlow}, \beta_{mlow})) \tag{6-13}$$

Figure Appendix A-0-3 illustrates 25 malicious users with the mixture coefficient $\gamma = 0.7$, meaning that the users follow the $Beta(\alpha_{mhigh}, \beta_{mhigh})$ in 70% sensing tasks (providing high quality data) and provide very low quality data in 30% sensing tasks (i.e., following the $Beta(\alpha_{mlow}, \beta_{mlow})$).

3. Trust-based, Average, and Polynomial Regression User Recruitment Schemes

```
Input:
  Initialize $N$ users
  Initialize $M$ service requests $R(i)$; $\forall i = \overline{1,M}$
  Initialize $R(i)$ comprised of $T_i$ sensing tasks;
  $ST_{R(i)}(j)$; $\forall j = \overline{1,T_\iota}$ , $\forall i = \overline{1,M}$ ;
  $ST_{R(i)}(j)$ is fulfilled by $P_{ij}$ participants $\forall j = \overline{1,T_\iota}$
Output:
  QoS scores for the M requests using different
  User Recruitment Schemes
```

- **Trust-based scheme:** establishes and maintains trust relationships between users based on the E-R trust model proposed in Section 6.4.2. It recruits users that have highest trust values with the service requester for the next sensing task.

```
Algorithm Trust-based
Initialize Trust[][], Exp[][], Rep[] /* Matrix of Trust, Experience, and Reputation */
out = 0; /* output: QoS scores for M requests */
for each R(i) from user u(i) in M requests do
  for each sensing task $ST_{R(i)}(j)$ in Ti tasks do
    Recruit $P_{ij}$ users with highest Trust[][u(i)]
    QoD_Assessment(collected data) from $P_{ij}$ users
    Update Exp[u(i)][$P_{ij}$]
    Update Rep[]
    Update Trust[][]
  out <- out + QoS(R(i))
return out
```

- **Average_QoD scheme**: calculates and maintains a list of the average QoD scores for each user based on data that the user has contributed in previous sensing tasks. It recruits users with highest average of QoD scores for the next sensing task.

```
Algorithm Average_QoD
Initialize AVG[] /*average QoD scores for users*/
out = 0; /*output: QoS scores for M requests */
for each R(i) from user u(i) in M requests do
  for each sensing task $ST_{R(i)}(j)$ in Ti tasks do
    Recruit $P_{ij}$ users with highest AVG[] scores
    QoD_Assessment(collected data) from $P_{ij}$ users
    Update AVG[] for the $P_{ij}$ users
  out <- out + QoS(R(i))
return out
```

- **Polynomial_Regression_QoD scheme:** maintains a list of the QoD scores for individual users in previous sensing tasks. A polynomial regression model is used to predict the QoD scores for the next sensing task; and users who have the highest predicted QoD scores are recruited. The 3-degree polynomial model by means of the least-square fit method is used as the predictive model in the algorithm.

```
Algorithm Polynomial_Regression_QoD
Initialize QoD_scores[][] /*QoD scores for all users in all previous sensing tasks*/
out = 0; /* output: QoS scores for M requests */
for each R(i) from user u(i) in M requests do
  for each sensing task $ST_{R(i)}(j)$ in Ti tasks do
    f = polyfit(t, QoD_scores[][],3)/*coefficients*/
    polyval(f, t+1) /*predict next QoD scores*/
    Recruit $P_{ij}$ users with highest predicted scores
    QoD_Assessment(collected data) from $P_{ij}$ users
    Update QoD_scores[][] for the $P_{ij}$ users
  out <- out + QoS(R(i))
return out
```

4. Data Usage Practical Expression and Prototype

DataItems:

A Data Item is an individual of Context Element container proposed in the NGSI 9/10 Information Model[20] used to exchange information about an entity, including entity ID, context attributes, related attribute domains, and metadata for all of the attribute values of the given domain. DataItem is formally defined in XML DTD syntax as follows.

```
<!DOCTYPE  TUCON[
<!ELEMENT  DataItem(ContextElement)>
<!ELEMENT  ContextElement(EntityID, AttributeDomainName?, ContextAttributeList, DomainMetadata?)>
<!ELEMENT  EntityID(Id,  Type)>
<!ELEMENT  ContextAttributeList(ContextAttribute*)>
<!ELEMENT  ContextAttribute(Name,  Type, ContextValue,  ContextMetadata+)>
<!ELEMENT  DomainMetadata(ContextMetadata*)>
<!ELEMENT  ContextMetadata(Name, Type, Value)>
...
```

[20] https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/NGSI-9/NGSI-10_information_model

```
]>
```

Authorizations:

TUCON policies represent constraints based on object attributes, subject attributes and conditions. The Authorizations optionally contains the following expressions: (i) ATT(O): Temporal Constraints for temporal granularity, Spatial Constraints for spatial granularity, and Abstraction Constraints for masking of certain information. (ii) ATT(S): Actor Type such as institutional, commercial operators, equipment manufacturers, or service providers, Monetization as the purpose of using data such as selling, training, or providing customer support. (iii) Conditions: trust value between data owner (trustor) and data consumers (trustee). Authorization XML DTD definition is as follows:

```
<!DOCTYPE  TUCON[
<!ELEMENT  Authorization(ATT_O*,  ATT_S*, Condition*)>
<!ELEMENT  ATT_O( Spatiality*, Temporality*,  Abstraction*)>
<!ELEMENT  ATT_S( Actor *, Monetization *)>
<!ELEMENT  Condition(Trust *)>
<!ELEMENT  Spatiality(SpatialScope*)>
<!ELEMENT  Temporality(TemporalScope*)>
<!ELEMENT  Abstraction(AbstractScope*)>
<!ELEMENT  Actor(ActorScope*)>
<!ELEMENT  Monetization(MonetizationScope*)>
<!ELEMENT  Trust(TrustScope*)>
<!ELEMENT  SpatialScope(Space?, Slot?, Street?, Zone?,  Any?)>
<!ELEMENT  TemporalScope(Hour?, Daily?,  Weekly?, Monthly?, Yearly?, Any?)>
<!ELEMENT  AbstractScope(Detail?, Statistical?, Any?)>
<!ELEMENT  TrustScope(Low, Medium, High?,  Any?)>
...
]>
```

Obligations:

This is a set of actions on DataItems such as Full Access, Partial Access, Dissemination, Storage, and Analysis. The Obligations are associated with Data Monetization, for example, if a data consumer requests for selling data, then Obligation action should be Dissemination; or if a data consumer requests for statistical training, then Obligation action should be Partial Access with constraints Temporality = {Weekly} & Abstraction = {Statistical}. XML DTD definition of Obligations is as follows:

```
<!DOCTYPE  TUCON[
<!ELEMENT  Obligations(Full?, Partly?, Dissemination?, Storage?, Analysis?)>
…
].
```

Access Rights:

Access Control decision is associated with Obligations and Authorization value. We simply define as Permission and Forbidden representing whether DataItems are allowed to “share” or not. The word “share” now can be more specifically understood in the TUCON context as: “allow to conduct appropriate obligation actions”. AccessRights is defined in XML DTD syntax as follows:

```
<!DOCTYPE  TUCON[
<!ELEMENT  AccessRight(Rule*)>
<!ELEMENT  Rule(Obligation?, Authorization?)>
…
]>
```

5. Smart Contract Pseudo-Code Example

Below is the pseudo-code of a Smart Contract for exchanging data with cryptocurrency (coin).

```
contract Data_Coin_Exchange {
    address public data_owner;
    address public coin_owner;
    event Sent_coin(address coin_owner, address data_owner, uint amount);
    function coin_receive(address data_owner, uint amount) {
        coin_balances[receiver] += amount;
    }
    function coin_deduct(address coin_owner, uint amount) {
        if (coin_balances[coin_owner] < amount) return;
        coin_balances[coin_owner] -= amount;
        coin_balances[data_owner] += amount;
        Sent_coin(coin_owner, data_owner, amount);
    }
    event Sent_data(address data_owner, address coint_owner, ownership
data_ownership);
    function data_receive(address coin_owner, ownership dataownership) {
        data_balances[receiver] += dataownership;
    }
    function dataownership_deduct(address data_owner, ownership dataownership) {
        if (data_balances[data_owner] <> data_ownership) return;
        data_balances[data_owner] -= data_ownership;
        data_balances[coin_owner] += data_ownership;
        Sent_data(data_owner, coin_owner, data_ownership);
    }
}
```

In this example, the Smart Contract defines terms and conditions under which the data buyer uses coin in exchange with data ownership. Once coin is sent from the coin_owner to the data_owner, the coin_balances of both data_owner and coin_owner are updated; and the data_balances which record data_ownerships are also updated accordingly. The transactions of digital money and data ownerships are recorded in Blockchain.

6. Smart Parking Service: Further Information

The Wise-IoT Smart Parking use case can be defined as an application based solution which, makes use of the available parking information from Busan and Santander cities, aiming to both demonstrate the interoperability of data between Europe and Korea through the Wise-IoT platform, and to provide a service to the users which suggests them a route to an empty parking lot in the city. A complete description of the use case can be found here[21]. Aiming to achieve the data interoperability, both data from Santander and Busan cities related to the smart parking service is designed in a concrete data model and is translated by the Wise-IoT Morphing Mediation Gateway before be finally stored in the Wise-IoT CIM layer.

In the case of Santander city, numerous parking sensors have been deployed in the downtown area to indicate the number of parking spots that are available or occupied. However, this will not be the only information to be provided to the user. As the Smart Parking use case embraces different functionalities which complement the main purpose of simply finding a parking lot in the city, different kinds of data will be required. For example, the Wise-IoT Recommendation System, which will be integrated within the use case, will provide guidance to the best area to park depending on different factors such as statistics of availability of free parking lots, traffic to arrive at it, crowd information, etc. So, as the interest is focused on providing an area instead of providing a concrete parking lot, it will be needed to define not only entities related to the parking lots but to parking areas. Besides, related to this use case, traffic monitoring data have to be defined in order to bring

[21] Wise-IoT D1.1 – Wise-IoT Pilot Use Case Technical Description, Business Requirements and Draft High-Level Architecture

inputs for the Recommendation System. This way, this data will be used to provide recommendations of parking areas avoiding those routes with higher occupation.

The instantiation, trust monitor, of the implementation and the integration of the trust management framework for Wise-IoT, providing inputs to the Self-Adaptive Recommender (SAR) (Self-Adaptive Recommender) as illustrated in Figure Appendix A-0-4. SAR is a system and set of components that implement the Self-Adaptation and Evolution perspective. As a system SAR has been developed as an approach to perform self-adaptation and evolution. It combines knowledge about the quality of context data and the users' behaviour and opinions to detect problems in the IoT system. It utilizes the combined knowledge such as trustworthiness of interacting entities to recommend to users how to best exploit the IoT system and to engineers how to improve the IoT system.

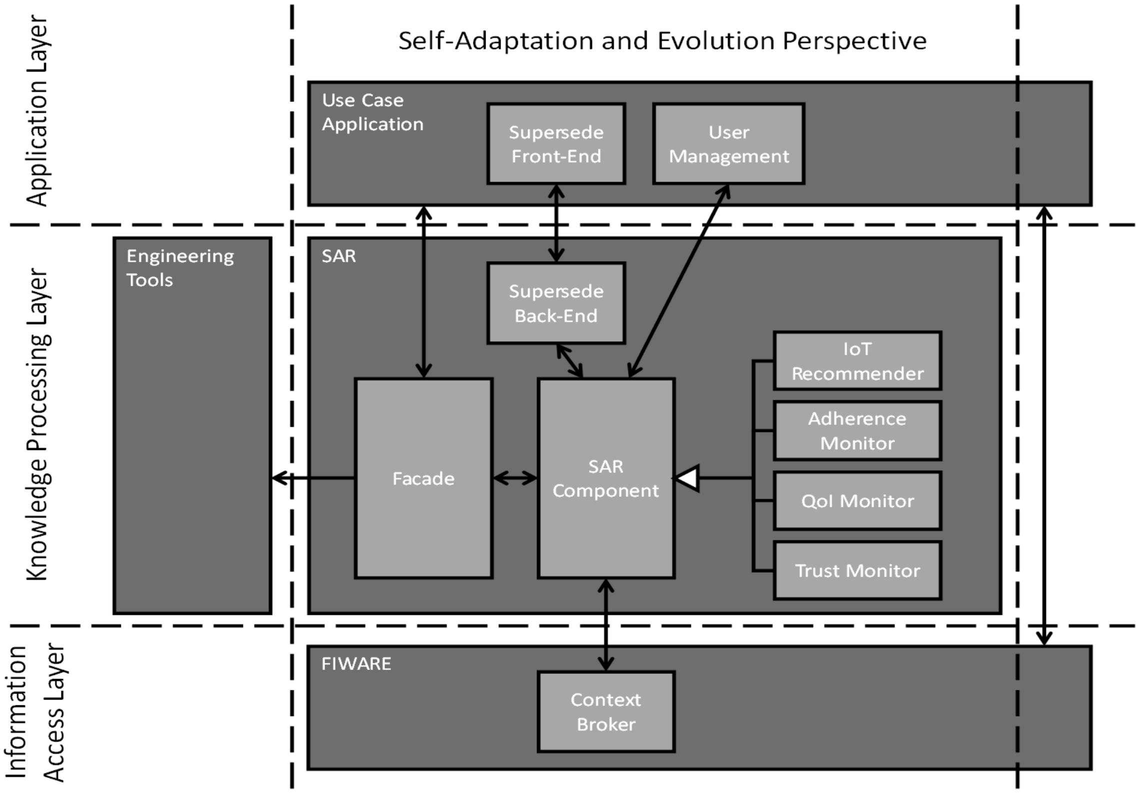


Figure Appendix A-0-4. Architecture of the Wise-IoT Self-Adaptive Recommender showing Trust Monitor Component.

The data model to be used to structure the information in the Smart Parking service in the Wise-IoT project will be the aforementioned NGSI, which will allow representing an entity (the parking lot, the parking area, traffic flow observation) by defining its entity id and its entity type. Also, the entity is defined with a set of attributes that represent the properties of the entity (*status*, *location*, *category*, *etc*.), defined by a name, a type and a value. Finally, each attribute can include metadata, which provides extra information about it (*timestamp*, *unit of measurement*, *etc*.). In addition, the underlying format to be used to represent this data structure is JSON. Regarding the semantic representation of information, FIWARE provides a Data Model, inspired by GSMA data models and schema.org, developed to produce harmonized schemas for the Internet of Things. In the case of parking information, the FIWARE Data Model specifies the semantic representation of all entities of interest: the parking spot, the parking area and the traffic information (*parkingSpot*, *OnStreetParking*, *TrafficFlowObserved* respectively). Starting with the definition of the *ParkingSpot* entity, the FIWARE Data Model provides a complete list of attributes for defining many parking spot characteristics. In addition, each of the attributes is described with its name, its description, its type and an indication about whether the attribute is mandatory or optional for the correct entity description. From this list, a concrete set of attributes have been selected to describe the resources deployed in the Santander facility: *identifier*, *type*, *dateModified*, *name*, *status*, *location*, *category* and *refParkingSite*.

7. Feedback Implementation and Usage in Smart Parking Service

To use the plugin, the use case application developer can copy the plugin folder into the directory where the web page (*html file*) resides, and add the following html code to the web page.

```
<!-- header -->
<link rel="stylesheet" href="dist/jqueryui/jquery-ui.min.css"/>
<link rel="stylesheet" href="dist/main.min.css"/>
<!-- footer -->
<script src="dist/jquery-3.2.1.js"></script>
<script src="dist/jqueryui/jquery-ui.min.js"></script>
<script src="dist/jquery.feedback.min.js"></script>
```

Then, when the application tells the SAR to finish the monitoring of a session, the SAR responds with the data needed for displaying the user feedback form. The data includes the form template and some additional parameters. After this, the form can be opened at any point in time, either upon an event, or it can be attached to an html element such as a button:

```
<script>
    $(document).ready(function () {
        ...
        //Option A: immediately open the feedback form
        jQuery(window).startDialogWithPullConfiguration({...});
        //Option B: attach the form to an html element
        jQuery('#button').startDialogWithPullConfigurationForElement({...});
        ...
    });
</script>
```

The function parameter {...} should look like the following example.

```
'apiEndpointOrchestrator': 'https://UrlToSarFacade/',
'apiEndpointRepository': 'https://UrlToSarFacade/',
'applicationPath': 'sar/service/AdherenceMonitor/feedbacks/formConfigs/',
'feedbackPath': 'sar/service/AdherenceMonitor/feedbacks/multipartform',
'applicationId': 9,
'pullConfigurationId': 34,
'goalEntityID': 'TestMyEntity',
'userId': '12345',
'lang': 'en',
'reviewActive': true
```

The first four lines contain paths to the API of the SAR façade, such that the plugin knows where it can get the form templates and where it must send the feedback to. The *applicationId* must be the same as the one in the Adherence Monitor configuration. The next three values (*pullConfigurationId*, *goalEntityID*, *userId*) need to be chosen according to the data from the SAR response. The *lang* field defines the language of the Supersede form elements, and *reviewActive* defines whether the feedback form should display an extra page or not where the user can review the feedback before submitting it.

Finally, styling options for displaying the feedback form are available in the included css file, or as additional fields in the function parameter. Android applications can now benefit from two frontend libraries that simplify the integration of the SAR system – a customized Supersede library for Wise-IoT and the SAR frontend library. The Supersede library for Android application is the equivalent of the Supersede *jQuery* plugin for web applications. Similar to the *jQuery* plugin, it can be used to trigger the display of a feedback form. But it does not automatically send the user feedback to the SAR, instead it returns the feedback to the application via a call-back. However, application developers do not need to know how the Supersede library works, because it gets encapsulated by the SAR frontend Android library. The SAR frontend library provides an easy-to-use Java API for all functionality related to the

SAR and the Supersede feedback. In its default configuration, the frontend library performs most of the work automatically and shields the developer from unnecessary details. It includes the following functionalities:

- It performs all RESTful API calls to the SAR façade.
- It provides call-back methods in case the developer needs to access the responses received from the SAR façade.
- It can automatically read the user's GPS position and send it to the SAR façade.
- It contains the part of the Trust Monitor that is responsible for user-specific trust scores.
- It takes care of storing SAR-related information, such as the session ID and the recommendation it receives, the user-specific trust scores, as well as the feedback form template data, and automatically re-uses the information where needed in the subsequent calls to the façade.
- It uses the feedback form template data when the application triggers the Supersede feedback mechanism, such that the application does not need to provide any additional parameters when triggering the mechanism. Further, it automatically sends the user feedback to the SAR façade when it is returned by the Supersede library.
- It contains various configuration options. For example, the use case application can decide whether user-specific trust scores should be sent to the SAR façade or not, and whether the library should use its own GPS mechanism or not.

Most of the exposed API methods have a synchronous and an asynchronous version. If the application chooses the asynchronous version, the library takes care of creating a new thread and running the code in the new thread. For responding, a call-back is used.

8. Deployment of the Trust Monitor Component in Smart Parking Service

The Trust Monitor component is deployed within the SAR system in WiseIoT project as following:

External Interfaces: The provided and required interfaces of the Trust Monitor are presented in Figure 58. The Trust Monitor basically takes QoI information of traffic sensors and parking sensors from the QoI component and Feedback from the Feedback from the Adherence Monitor component as its inputs for the trust evaluation process. As can be seen in Figure Appendix A-0-5, the Trust Monitor provides an API to the IoT Recommender for enquiring about the trust evaluation value (or trust score) between two any entities (i.e., users and parking spots).

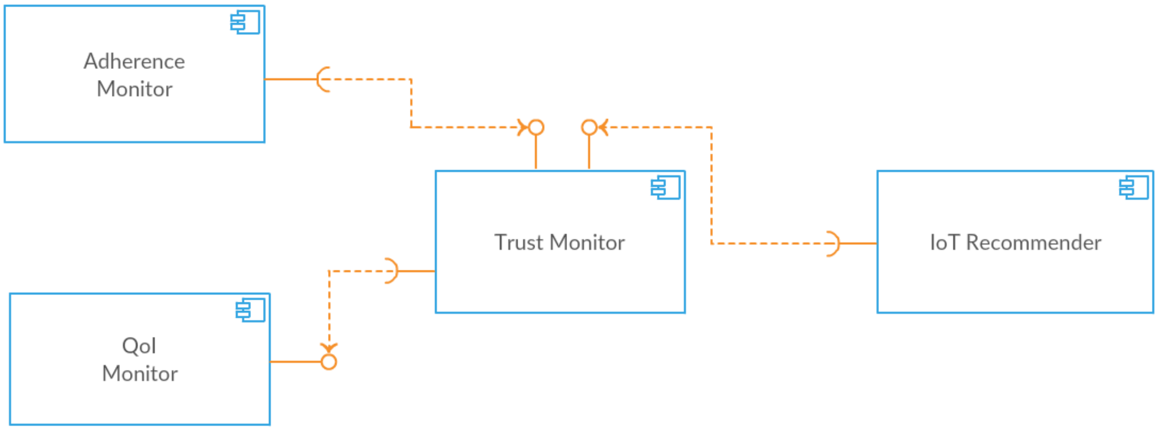


Figure Appendix A-0-5. UML Diagram for the Trust Monitor External Interface

API and Data Model: The Trust Monitor provides two RESTful APIs for the Adherence Monitor to submit users' feedback as well as for the IoT Recommender to obtain trust values between users and parking spots.

Provided API to Adherence Monitor: The Trust Monitor subscribes to the Context Broker and whenever a user submits a feedback about the parking place that the user has just used, the Adherence Monitor will send the feedback information to the Trust Monitor using the provided API. For providing the API, the following RESTful API method is used. The response to the method call includes the acknowledgement for the feedback transfer as being successful or unsuccessful.

```
GET  http://ip.to.the.service:port/TrustMonitor/fbsubmit?UID=user_id&
PSID=urn:entity:santander:parking:parkingSpot:3601&value=feedback_score&timestamp=time
```

- *Query parameters*:

UID is the *user_id* which is set from 1 to 100. The real *user_id* for the Brussels demo is 1.

PSID is the parking place ID which is from *urn:entity:santander:parking:parkingSpot:3601* to *urn:entity:santander:parking:parkingSpot:3923*

value is the feedback score which is normalized to the range [0-1]

timestamp is the timestamp when the user submits the feedback, which is converted in to *Java.DataTime (type: long)*

- *Response status*:

status 0 if the feedback submission is not successful and 0 otherwise. It is in form of JSON object

```
Headers: Content-Type: application/json, Accept: application/json
Body:
{
    "id":11,
    "user_id":"user_id",
    "parking_place_id":"parking_place_id",
    "feedback_score":0.51,
    "timestamp":1499003993933,
    "status":0, //if successful or 1 if unsuccessful
}
```

Provided API to the IoT Recommender Monitor: The Trust Monitor provides the RESTful API to the IoT Recommender that when the IoT Recommender needs to get the trust value between a user and a parking spot, it will request through the API by providing the *User_id* and *parking_place_ID* parameters. The response to the method call includes the JSON object as the output containing the information about the trustor (user), the trustee (parking spot), the trust score between the two, and the timestamp of the request.

```
POST  http://ip.to.the.service:port/TrustMonitor/trustrequest?UID=user_id&
PSID=urn:entity:santander:parking:parkingSpot:3601
```

- *Query parameters*:

UID is the *user_id* which is set from 1 to 100. The real *user_id* for the Brussels demo is 1.

PSID is the *parking place ID* which is from *urn:entity:santander:parking:parkingSpot:3601* to *urn:entity:santander:parking:parkingSpot:3923*

- *Response message*:

The API response as a JSON object containing the trust value information between the user and the parking place specified in the requested parameters.

```

Headers: Content-Type: application/json, Accept: application/json
Body:
{
    "id":11,
    "trustorId":"user_id",
    "trusteeId":"parking_place_id",
    "score":0.51,
    "timestamp":1499003993933
}
```

score is the trust value which is normalized to the range [0-1] *timestamp* is the timestamp when the user submits the feedback, which is converted in to *Java.DataTime (type: long)*

Requested API from QoI Monitor: The Trust Monitor needs QoI information for evaluating trust value, thus the QoI Monitor should provide a RESTful API so that whenever the Trust Monitor gets a request from IoT Recommender, it will start to evaluate the trust score by enquiring the QoI Monitor for the QoI value of the parking sensors in the parking places. Note that the parking place ID is used interchangeably with the parking sensor ID. Therefore, there is no difference between the parking places and the parking sensors.

```
POST
http://ip.to.the.service:port/QoIMonitor/QoIRequest?PSID=urn:entity:santander:parking:
parkingSpot:3601
```

- *Query parameters*:

PSID is the parking place ID which is *from urn:entity:santander:parking:parkingSpot:3601* to *urn:entity:santander:parking:parkingSpot:3923*

Response message: It should be in form of JSON object as following

```
Headers: Content-Type: application/json, Accept: application/json

Body:

{

    "parking_place_id":"parking_place_id",

    "QoI_score":0.51,

    "timestamp":1499003993933,

}
```

score is the QoI value which is normalized to the range [0-1]

timestamp is the timestamp when the QoI Monitor responses to the requests for the QoI value of the parking place from the Trust Monitor, which is converted in to *Java.DataTime (type: long)*

Behaviour (Interaction between Trust Monitor-related components): The sequence diagram in Figure Appendix A-0-6 shows how the Trust Monitor interacts with the SAR components including Adherence Monitor, QoI Monitor and the IoT Recommender during a monitoring session as well as when an event occurs (i.e., request from the IoT Recommender for trust evaluation).

- The Adherence Monitor sends the feedback information to the Trust Monitor whenever a user submits a feedback about the parking spot she/he has just used; and the Trust monitor responds with the Acknowledgement whether the feedback information transmission is successful or not. This event is independent from other interactions with the QoI Monitor and the IoT Recommender.

- When the IoT Recommender needs to recommend a parking spot to a user, it will send a request for trust evaluation between the user and the parking spot through the provided Trust Monitor API with UserID and Parking Spot ID parameters. The Trust Monitor receives the request from the IoT Recommender, it will ask the QoI Monitor component for the QoI value of the parking sensor which is deployed at the parking spot. The QoI information is a kind of real time monitoring and will respond with the real time QoI value for the parking sensor. Then the Trust Monitor will evaluate the value between the user and the parking spot by conducting its algorithms and mechanisms before sending the response in JSON object to the IoT Recommender. The IoT Recommender will look for the trust value in the received JSON object and use it in making a decision for the recommendation.

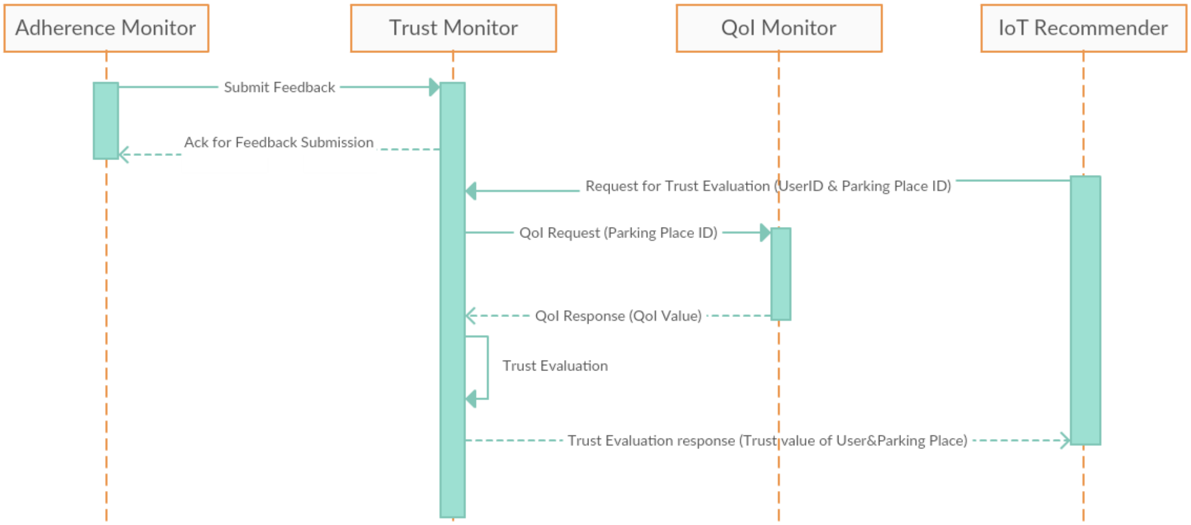

Adherence Monitor
Trust Monitor
QoI Monitor
IoT Recommender
Submit Feedback
Ack for Feedback Submission
Request for Trust Evaluation (UserID & Parking Place ID)
QoI Request (Parking Place ID)
QoI Response (QoI Value)
Trust Evaluation
Trust Evaluation response (Trust value of User&Parking Place)

Figure Appendix A-0-6. Trust Monitor's collaboration with Adherence Monitor, QoI Monitor, and IoT Recommender

- Deployment: The Trust Monitor is implemented using REST Web service for providing as well as receiving RESTful APIs. The trust algorithms and mechanisms are implemented locally with a local database using *MongoDb* as a standalone web service. The software component using a WAR file will be provided, which can be easily deployed into the Docker container. For the *MongoDb* database, there are two approaches for the integration. We could provide a migration mechanism for migrating *MongoDb* database into the Wise-IoT database. Otherwise, a URI can be provided for the database; and then the trust monitor web service can be deployed on a global server (i.e., Wise-IoT server) and remotely access the database for the provided APIs. The configuration for web server as well as for the database server is easily achieved by modifying some parameters set in the file*: /src/main/resources/application.properties* as follows:

```
server.address= #Network address to which the server should bind to.
server.port=8080 #Server HTTP port.
server.server-header= #Value to use for the Server response header (no header is sent
if empty)
server.servlet-path=/ #Path of the main dispatcher servlet.

spring.data.mongodb.database=test
spring.data.mongodb.uri
spring.data.mongodb.username
spring.data.mongodb.password
spring.data.mongodb.host=localhost #Mongo server host.Cannot be set with uri.
spring.data.mongodb.repositories.enabled=true #Enable Mongo repositories.
```

APPENDIX B: SOURCE CODE AND PROGRAMS

I have developed variety of implementation both in Matlab for demonstrating the proposed trust-related algorithms and mechanisms in our papers; as well as in Java for software development during the time participating two project TII and Wise-IoT.

It seem useless if I write down the source-code in this thesis as references. Instead, I have uploaded all the source-code to my personal Github. Information and source-code can be found in this link[22], referring the document files in each Github repository for more detail.

APPENDIX C: STANDARDIZATION

ITU-T SG20 FG-DPM meeting (Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities, Brussels, Belgium, 20-23 February 2018)

[ts-1] **Nguyen B. Truong**, Yuanfang Chen, Hyunwoo Lee, "Proposal for D3.6 – Anonymity and Privacy on the Blockchain", April 2018.

ITU-T FG-DPM meeting (Geneva, 20-25 October 2017)

[22] https://github.com/nguyentb/

[ts-1] **Nguyen B. Truong**, Kassem Hayatt, Hamza Baqa, "Proposal for D4.4 – Overview of Data Quality Management," DPM-I-88, October 2017.

[ts-2] **Nguyen B. Truong**, Kassem Hayatt, Hamza Baqa, "Proposal for D4.4 – Overview of Data Quality Measurement," DPM-I-89, October 2017.

[ts-3] **Nguyen B. Truong**, Kassem Hayatt, Hamza Baqa, "Proposal for D4.4 – Categorization on Data Quality Dimensions," DPM-I-90, October 2017.

[ts-4] **Nguyen B. Truong**, Kassem Hayatt, Hamza Baqa, "Proposal for D4.4 - Data Quality Dimensions in Details," DPM-I-91, October 2017.

[ts-5] **Nguyen B. Truong**, Kassem Hayatt, Hamza Baqa, "Proposal for D4.4 - Data Quality Problems," DPM-I-92, October 2017.

ITU-T SG13 meeting (Geneva, 6 – 17 February 2017)

[ts-13] Upul Jayasinghe, **Nguyen B Truong**, Gyu Myoung Lee, Hyunwoo Lee, "Proposal for indirect trust in Clause 7.1 of Y.trust-provision," SG13-C.0138, January 2017.

[ts-14] **Nguyen B. Truong**, Upul Jayasinghe, Gyu Myoung Lee, Cheol-hye Cho, "Proposal for for detailed trust analysis in a specific trust provisioning use case," SG13-C.0139, January 2017.

ITU-T SG13 Q11 and Q16 interim meeting (e-meeting, 30 August – 1 September 2016)

[ts-18] **Nguyen B. Truong**, Gyu Myoung Lee, Tai-Won Um, "Proposed revisions of Appendix II in Y.trust-provision," Q16-13-Aug16-C-49, August 2016.

ITU-T SG13 meeting (Geneva, 27 June – 8 July 2016)

[ts-29] **Nguyen B. Truong**, Gyu Myoung Lee, Tai-Won Um, Hyunwoo Lee, "Proposal on key features of trust in ICT infrastructures," COM13-C1400-E, June 2016.

[ts-30] **Nguyen B. Truong**, Gyu Myoung Lee, Tai-Won Um, Hyunwoo Lee, "Proposal on potential risks in ICT infrastructures," COM13-C1401-E, June 2016.

ITU-T SG13 meeting (Geneva, 30 November – 11 December 2015)

[ts-36] **Nguyen B. Truong**, Gyu Myoung Lee, Tai-Won Um, Hyunwoo Lee, "Proposal for Section 2 on understanding of trust in CG-Trust Technical Report," COM13C-1095-E, November 2015.

REFERENCES

[1] G. Xiong, F. Zhu, X. Liu, X. Dong, W. Huang, S. Chen*, et al.*, "Cyber-physical-social system in intelligent transportation," *IEEE/CAA Journal of Automatica Sinica,* vol. 2, pp. 320-333, 2015.

[2] A. Sheth, P. Anantharam, and C. Henson, "Physical-Cyber-Social Computing: An Early 21st Century Approach," *IEEE Intelligent Systems,* pp. 78 - 82, 2013.

[3] L. Atzori, A. Iera, and G. Morabito, "Siot: Giving a social structure to the internet of things," *IEEE communications letters,* vol. 15, pp. 1193-1195, 2011.

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

[5] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks,* vol. 76, pp. 146-164, 2015.

[6] P. N. Mahalle, P. A. Thakre, N. R. Prasad, and R. Prasad, "A fuzzy approach to trust based access control in internet of things," in *Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE),* Atlantic City, NJ, June 2013.

[7] A. Josangl, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems,* pp. 618-644, March 2007

[8] L. Page, Brin, S., Motwani, R., & Winograd, T. , "The PageRank Citation Ranking: Bringing Order to the Web," Stanford InfoLab1998.

[9] Y. Atif, "Building trust in e-commerce," *IEEE Internet Computing,* vol. 6, pp. 18 - 24, Feb., 2002.

[10] X. Li and L. Liu, "A reputation-based trust model for peer-to-peer e-commerce communities," in *IEEE International Conference on E-Commerce,* New York, USA, 2003, pp. 275-284.

[11] F. Bao and I. Chen, "Trust Management for Internet of Things and its Application to Service Composition," in *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM),* USA, 2012.

[12] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *Journal of network and computer applications,* vol. 35, pp. 867-880, 2012.

[13] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: A survey," *IEEE Communications Surveys & Tutorials,* vol. 14, pp. 279-298, 2012.

[14] J. H. Cho, A. Swami, and R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys & Tutorials,* vol. 13, pp. 562-583, 2011.

[15] J. Li, R. Li, and J. Kato, "Future trust management framework for mobile ad hoc networks," *IEEE Communications Magazine,* vol. 46, 2008.

[16] S. Kraounakis and e. al., "A Robust Reputation-Based Computational Model for Trust Establishment in Pervasive Systems," *IEEE Systems Journal,* pp. 878-891, 2015.

[17] B. Guo, Z. Wang, Z. Yu, Y. Wang, N. Y. Yen, R. Huang*, et al.*, "Mobile crowd sensing and computing: The review of an emerging human-powered sensing paradigm," *ACM Computing Surveys (CSUR),* vol. 48, 2015.

[18] B. Alcalde, "Towards a Decision Model based on Trust and Security Risk Management," *Seventh Australasian Conference on Information Security,* pp. 61-67, 2009.

[19] uTRUSTit-2012, "White Paper: Trust Definition "Defining, Understanding, Explaining TRUST within the uTRUSTit Project", August 2012.," 2012.

[20] Z. Yan and C. Prehofer, "Autonomic Trust Management for a Component based Software System," *IEEE Transactions Dependable Secure Computing,* pp. 810-823, 2011.

[21] Z. Yan, Zhang, P., Vasilakos, A. V. , "A Survey on Trust Management for Internet of Things," *Journal of Network and Computer Applications,* pp. 120-134, 2014.

[22] D. Gambetta, "Can We Trust Trust," in *Trust: Making and Breaking Cooperative Relations,* ed, 1990, pp. 213-238.

[23] M. S. T. Grandison, "A Survey of Trust in Internet Applications," *IEEE Communications Surveys and Tutorials*, 2009.

[24] G. S. Ilung Pranata, Rukshan Athauda, "A Holistic Review on Trust and Reputation Management Systems for Digital Environments," *International Journal of Computer and Information Technology*, vol. 1, pp. 2277 – 0764, September 2012 2012.

[25] E. Chang, F. K. Hussain, and T. S. Dillon, "Fuzzy nature of trust and dynamic trust modelling in service oriented environments," in *Workshop on secure web services*, Fairfax, USA, 2005.

[26] E. Chang, T. Dillon, and F. K. Hussain, "Trust Reputation for Service-Oriented Environments," ed West Sussex, England: John Wiley & Sons Ltd, 2006.

[27] J. F. M. Blaze, J.Lacy, "Decentralized trust management," in *Proceedings of IEEE Conference on Security and Privacy*, 1996.

[28] N. Li and J. C. Mitchell, "Datalog with Constraints: A Foundation for Trust-management Languages," in *Proceedings of the Fifth International Symposium on Practical Aspects of Declarative Languages*, 2003.

[29] R. Lacuesta, Palacios-Navarro, G., Cetina, C., Peñalver, L.,Lloret, J., "Internet of Things: Where to be is to Trust " *EURASIP Journal on Wireless Communications and Networking*, pp. 1-16, 2012.

[30] P. N. Mahalle, Thakre, P.A., Prasad, N.R., Prasad, R., "A Fuzzy Approach to Trust Based Access Control in Internet of Things," in *Wireless Communications, Vehicular Technology, Information Theory and Aerospace and Electronic Systems*, 2013.

[31] T. Beth, Borcherding, M., Klein, B., "Valuation of trust in open networks," in *European Symposium on Research in Computer Security*, 1994.

[32] G. Caronni, "Walking the web of trust," in *Proceedings of 9th IEEE International Workshops on Enabling Technologies (WETICE)*, 2000.

[33] P. Cofta, *Front Matter*: Wiley Online Library, 2007.

[34] C. N. Ziegler, Lausen G., "Propagation models for trust and distrust in social networks," *Information Systems Frontiers*, vol. 7, pp. 337-358, 2005.

[35] J. P. Wang, S. Bin, Y. Yu, and X. X. Niu, "Distributed Trust Management Mechanism for the Internet of Things," *Applied Mechanics and Materials (Appl. Mech. Mater.)*, pp. 2463-2467, Aug. 2013.

[36] N. Palaghias, N. Loumis, S. Georgoulas, and K. Moessner, "Quantifying trust relationships based on real-world social interactions," in *IEEE International Conference on Communications (ICC)*, Kuala Lumpur, Malaysia, 2016.

[37] A. B. Can and B. Bhargava, "Sort: A self-organizing trust model for peer-to-peer systems," *IEEE transactions on dependable and secure computing*, vol. 10, pp. 14-27, 2013.

[38] W. S. Sherchan, Nepal, and C. Paris, "A survey of trust in social networks," *ACM Computing Surveys (CSUR)*, vol. 45, 2013.

[39] F. Bao and I. Chen, "Dynamic Trust Management for Internet of Things Applications," in *International Workshop on Self-Aware Internet of Things (Self-IoT)*, USA, 2012.

[40] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, "A Subjective Model for Trustworthiness Evaluation in the Social Internet of Things," in *IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC)*, Australia, 2013.

[41] P. B. Velloso, R. P. Laufer, D. O. Cunha, O. Duarte, and G. Pujolle, "Trust management in mobile ad hoc networks using a scalable maturity-based model," *IEEE transactions on network and service management* vol. 7, pp. 172-185, 2010.

[42] S. Brin and L. Page, "Reprint of: The anatomy of a large-scale hypertextual web search engine," *Computer Networks*, vol. 56, pp. 3825–3833, 2012.

[43] C. A. H. Pramod Anantharam, Krishnaprasad Thirunarayan, Amit P. Sheth, "Trust Model for Semantic Sensor and Social Networks: A Preliminary Report," in *Aerospace and Electronics Conference (NAECON)*, Ohio, US, 2010.

[44] S. P. Marsh, "Formalising trust as a computational concept," 1994.

[45] P. Zimmermann, "Pretty good privacy user’s guide," *Distributed with PGP software*, vol. 1, 1993.

[46] P. Samarati and P. Bonatti, "Regulating service access and information release on the web," in *7th ACM conference on computer and communications security*, 2000.

[47] N. Li and J. Mitchell, "RT: A Role-based Trust-management Framework," in *DARPA Information Survivability Conference and Exposition (DISCEX)*, Washington D.C, 2003.

[48] R. Gavriloaie, W. Nejdl, D. Olmedilla, K. E. Seamons, and M. Winslett, "How to use declarative policies and negotiation to access sensitive resources on the semantic web," in *1st European Semantic Web Symposium (ESWS)*, Crete, Greece, 2004.

[49] P. A. Bonatti and D. Olmedilla, "Driving and monitoring provisional trust negotiation with metapolicies," in *IEEE 6th International Workshop on Policies for Distributed Systems and Networks (POLICY)*, Stockholm, Sweden, 2005.

[50] M. Winslett, T. Yu, K. E. Seamons, A. Hess, J. Jacobson, R. Jarvis*, et al.*, "Negotiating trust on the web," *IEEE Internet Computing*, pp. 30-37, 2002.

[51] J. Kohl and C. Neuman, "The Kerberos network authentication service," IETF RFC 15101993.

[52] W. H. Winsborough, K. E. Seamons, and V. E. Jones, "Automated trust negotiation," in *Proceedings of theDARPAInformation Survivability Conference*, 2000, pp. 88-102.

[53] T. Yu and M. Winslett, "Policy migration for sensitive credentials in trust negotiation," in *Proceedings of the 2003 ACM Workshop on Privacy in the Electronic Society (WPES 03)*, New York, USA, 2003, pp. 9-20.

[54] T. Yu, M. Winslett, and K. E. Seamons, "Interoperable Strategies in Automated Trust Negotation," in *Proceedings of the 8th ACM Conference on Computer and Communications Security*, New York, USA, 2001, pp. 146–155.

[55] W. Nejdl, D. Olmedilla, and M. Winslett, "Peertrust: automated trust negotiation for peers on the semantic web,," in *Proceedings of Workshop on Secure Data Management in a Connected World in Conjunction with the 30th International Conference on Very Large Data Bases*, 2004, pp. 118–132.

[56] N. Li, W. H. Winsborough, and J. C. Mitchell, "Distributed credential chain discovery in trust management," *Computer Security 11,* pp. 35-86, 2003.

[57] J. M. Seigneur and C. D. Jensen, "Trust enhanced ubiquitous payment without too much privacy loss," in *Proceedings of the 2004 ACM Symposium on Applied Computing*, New York, USA, 2004, pp. 1593–1599.

[58] F. L. Gandon and N. M. Sadeh, "Semantic web technologies to reconcile privacy and context awareness," in *UbiMob '04: Proceedings of the 1st French-speaking Conference on Mobility and Ubiquity Computing*, New York, USA, 2004, pp. 123–130.

[59] A. Uszok, J. Bradshaw, R. Jeffers, N. Suri, P. Hayes, M. Breedy*, et al.*, "Kaos policy and domain services: toward a description-logic approach to policy representation, deconfliction, and enforcement policy," in *POLICY '03 Proceedings of the 4th IEEE International Workshop on Policies for Distributed Systems and Networks*, Washington DC, USA, 2003.

[60] L. Kagal, T. W. Finin, and A. Joshi, "A policy-based approach to security for Semantic Web," in *Proceedings of the 2nd International Semantic Web Conference*, 2003, pp. 402–418.

[61] M. Nielsen and K. Krukow, "Towards a formal notion of trust," in *Proceedings of the 5thACMSIGPLAN International Conference on Principles and Practice of Declaritive Programming*, New York, USA, 2003.

[62] OASIS, "WS-Trust 1.4," in *WS-Trust 1.4*, ed, 2012.

[63] M. Carbone, M. Nielsen, and V. Sassone, "A formal model for trust in dynamic networks," in *Proceedings of International Conference on Software Engineering and Formal Methods*, 2003.

[64] M. Y. Becker and P. Sewell, "Cassandra: Distributed access control policies with tunable expressiveness," in *International Workshop on Policies for Distributed Systems and Networks*, 2004.

[65] T. Leithead, Nejdl, W., Olmedilla, D., Seamons, K. E., Winslett, M., Yu, T., Zhang, C. C., "How to exploit ontologies for trust negotiation," in *Workshop on Trust, Security, and Reputation on the Semantic Web (ISWC)*, 2004.

[66] J. F. M. Blaze, J. Lacy, "Decentralized trust management," in *Proceedings of IEEE Symposium on Security and Privacy*, 1996, pp. 164-173.

[67] M. Blaze, Feigenbaum, J., Keromytis, A. D. , "KeyNote: Trust management for public-key infrastructures," in *International Workshop on Security Protocols*, 1998.

[68] L. Xiong and L. Liu, "A Reputation-based Trust Model for Peer-to-Peer E-Commerce Communities," in *IEEE International Conference on E-Commerce Technology (CEC)*, 2003, pp. 275-284.

[69] P. Resnick, Kuwabara, K., Zeckhauser, R., Friedman, E. , "Reputation Systems " *Communications of the ACM*, pp. vol. 43, pp. 45-48, 2000.

[70] A. Abdul-Rahman, Hailes, S., "A distributed trust model," in *The New Security Paradigms Workshop*, 1997, pp. 48–60.

[71] A. Abdul-Rahman, Hailes, S., "Using recommendations for managing trust in distributed systems," in *Proceedings of IEEE International Conference on Communication*, 1997.

[72] B. Yu, Singh, M. P., "A social mechanism of reputation management in electronic communities," in *International Workshop on Cooperative Information Agents*, London, UK, 2000, pp. 154–165.

[73] B. Yu, Singh, M. P., "An evidential model of distributed reputation management," in *AAMAS '02: Proceedings of the First International Joint Conference onAutonomousAgents and Multiagent Systems*, New York, USA, 2002, pp. 294–301.

[74] B. Yu, Singh, M. P., "Detecting deception in reputation management," in *AAMAS '03: Proceedings of the Second International Joint Conference on Autonomous Agents and Multiagent Systems*, New York, USA, 2003, pp. 73–80.

[75] J. Sabater, Sierra, C., "Reputation and social network analysis in multiagent systems," in *AAMAS '02: Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems*, New York, USA, 2002.

[76] S. Brin, Page, L., "The anatomy of a large-scale hypertextual Web search engine," *Computer Networks,* pp. 107–117, 1998.

[77] S. D. Kamvar, Schlosser, M. T., Garcia-Molina, H. , "The eigentrust algorithm for reputation management in P2P networks," in *12th International Conference on World Wide Web,* New York, NY, USA, 2003.

[78] E. Damiani, di Vimercati, D. C., Paraboschi, S., Samarati, P., Violante, F., "A reputation-based approach for choosing reliable resources in peer-to-peer networks," in *9th ACM Conference on Computer and Communications Security*, New York, NY, USA, 2002.

[79] J. Golbeck, Hendler, J., "Accuracy of metrics for inferring trust and reputation," in *Proceedings of the 14th International Conference on Knowledge Engineering and Knowledge Management*, 2004.

[80] J. Golbeck, Hendler, J., "Inferring reputation on the semantic web," in *Proceedings of the 13th InternationalWorldWideWeb Conference*, 2004.

[81] P. Massa, Avesani, P., "Controversial users demand local trust metrics: an experimental study on epinions.com community," in *25th American Association for Artificial Intelligence Conference*, 2005.

[82] P. A. Chirita, Nejdl, W., Schlosser, M. T., Scurtu, O., "Personalized reputation management in P2P networks," in *Proceedings of the Trust, Security and Reputation Workshop Held at the 3rd International Semantic Web Conference*, 2004.

[83] F. Bao, Chen, I. R., "Dynamic Trust Management for the Internet of Things Applications," in *International Workshop on Self-Aware Internet of Things,* San Jose, USA, 2012.

[84] F. Bao, Chen, I. R., "Trust Management for the Internet of Things and Its Application to Service Composition," in *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, Francisco, USA, June 2012.

[85] D. Chen, Chang, G., Sun, D., Li, J., Jia, J., Wang, X., "TRM-IoT: a trust management model based on fuzzy reputation for Internet of Things," *Computer Science and Information Systems,* vol. 8, pp. 1207-1228, 2011.

[86] N. B. Truong, Um, T. W., Lee, G. M., "A Reputation and Knowledge Based Trust Service Platform for Trustworthy Social Internet of Things," in *Innovations in Clouds, Internet and Networks (ICIN)*, Paris, France, March 2016.

[87] A. Jøsang, "A logic for uncertain probabilities," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems,* vol. 9, pp. 279– 311, June 2001.

[88] A. Jøsang, Ismail, R., Boyd, C. , "A survey of trust and reputation systems for online service provision," *Decision Support Systems,* 2007.

[89] F. Bao, Chen, R., Guo, J., "Scalable, Adaptive and Survivable Trust Management for Community of Interest Based Internet of Things Systems," in *11th International Symposium on Autonomous Decentralized System*, Mexico City, Mexico, 2013.

[90] R. Chen, Guo, J., "Dynamic Hierarchical Trust Management of Mobile Groups and Its Application to Misbehaving Node Detection," in *International Conference on. Advanced Information Networking and Applications*, Victoria, Canada, 2014.

[91] B. Alcalde, Dubois, E., Mauw, S., Mayer, N., Radomirović, S., "Towards a Decision Model based on Trust and Security Risk Management," in *The Seventh Australasian Conference on Information Security*, Wellington, New Zealand, 2009, pp. 61-70.

[92] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, "Not so different after all: A cross-discipline view of trust," *Academy of management review,* vol. 3, pp. 393-404, 1998.

[93] K. Thompson, "Reflections on trusting trust," *Communications of the ACM,* vol. 27, pp. 761-763, 1984.

[94] N. B. Truong, Q. H. Cao, T. W. Um, and G. M. Lee, "Leverage a trust service platform for data usage control in smart city," in *IEEE Global Communications Conference (GLOBECOM),* Washington DC, U.S.A, December, 2016.

[95] T. Grandison and M. Sloman, "A survey of trust in internet applications," *IEEE Communications Surveys & Tutorials,,* vol. 3, pp. 2-16, 2000.

[96] J. D. Lewis and A. Weigert, "Trust as a social reality," *Social forces,* vol. 63, pp. 967-985, 1985.

[97] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *Academy of management review,* vol. 20, pp. 709-734, 1995.

[98] NIST, "Managing Information Security Risk: Organization, Mission, and Information System View," U.S. Department of Commerce, Gaithersburg, MD, United States2011.

[99] Z. Yan, W. Ding, V. Niemi, and A. V. Vasilakos, "Two schemes of privacy-preserving trust evaluation," *Future Generation Computer Systems,* vol. 62, pp. 175-189, 2016.

[100] N. B. Truong, H. Lee, B. Askwith, and G. M. Lee, "Toward a Trust Evaluation Mechanism in the Social Internet of Things," *SENSORS,* vol. 17, 2017.

[101] I. Chen, F. Bao, and J. Guo, "Trust-based Service Management for Social Internet of Things Systems," *IEEE Transactions on Dependable and Secure Computing,* pp. 1-14, 2015.

[102] M. Al-Kuwaiti, N. Kyriakopoulos, and S. Hussein, "A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability," *IEEE Communications Surveys & Tutorials,* vol. 11, pp. 106 - 124, 2009.

[103] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "For Computing and its role in the Internet of Things," in *ACM Workshop on Mobile Computing MCC*, New York, USA, Aug., 2012.

[104] U. Jayasinghe, N. B. Truong, T. W. Um, and G. M. Lee, "RpR: A trust computation model for social Internet of Things," in *IEEE Smart World Congress*, Toulouse, France, 2016

[105] R. Kumar, S. A. Khan, and R. A. Khan, "Revisiting software security: durability perspective," *International Journal of Hybrid Information Technology (SERSC),* vol. 8, pp. 311-322, 2015.

[106] NIST, "Cyber-Physical Systems (CPS) Framework Release 1.0," US Department of Commerce, Gaithersburg, MD, USA2016.

[107] S. Santini and R.Jain, "Similarity measures," *IEEE Transactions on pattern analysis and machine Intelligence,* vol. 9, pp. 871-883, 1999.

[108] G. Klir and B. Yuan, *Fuzzy sets and fuzzy logic* vol. 4: Prentice hall New Jersey, 1995.

[109] L. A. Zadeh, "Fuzzy logic, neural networks, and soft computing," *Communications of the ACM,* vol. 37, pp. 77-85, 1994.

[110] L. A. Zadeh, "Fuzzy logic= computing with words," *IEEE transactions on fuzzy systems,* vol. 4, pp. 103-111, 1996.

[111] E. H. Mamdani, "Application of fuzzy algorithms for control of simple dynamic plant," *Electrical Engineers, Proceedings of the Institution of,* vol. 121, pp. 1585-1588, 1974.

[112] M. Sugeno, *Industrial applications of fuzzy control*: Elsevier Science Inc., 1985.

[113] A. Hamam and N. D. Georganas, "A comparison of Mamdani and Sugeno fuzzy inference systems for evaluating the quality of experience of Hapto-Audio-Visual applications," in *Haptic Audio visual Environments and Games, 2008. HAVE 2008. IEEE International Workshop on*, 2008, pp. 87-92.

[114] T. Berners-Lee, "Linked Data," *International Journal on Semantic Web and Information System, W3C,* vol. 4, 2006.

[115] O. Hartig, C. Bizer, and J. C. Freytag, "Executing SPARQL Queries over the Web of Linked Data," in *ISWC '09 Proceedings of the 8th International Semantic Web Conference,* Washington DC, 2009, pp. 293-309.

[116] S. J. Russell and P. Norvig, "Knowledge and Reasoning," in *Artificial Intelligence: A Modern Approach,* ed New Jersey: Prentice Hall, 2014, pp. 149-297.

[117] F. Baader, D. Calvanese, D. L. McGuinness, D. Nardi, and P. F. Patel-Schneider, *The description logic handbook: theory, implementation, and applications*. New York, NY, USA: Cambridge University Press, 2003.

[118] K. Simon and C. Malcolm, *An Introduction to Knowledge Engineering*. New York, NY, USA: Springer-Verlag 2006.

[119] R. F. Baumeister and M. R. Leary, "The need to belong: desire for interpersonal attachments as a fundamental human motivation," *Psychological bulletin,* vol. 3, p. 497, 1995.

[120] D. L. Oswald, E. M. Clark, and C. M. Kelly, "Friendship maintenance: An analysis of individual and dyad behaviors," *Journal of Social and Clinical Psychology,* vol. 3, pp. 413-441, 2004.

[121] S. G. Roberts, R. I. Dunbar, T. V. Pollet, and T. Kuppens, "Exploring variation in active network size: Constraints and ego characteristics," *Social Network,* vol. 31, pp. 138-146, 2009.

[122] S. Kamvar and M. Schlosser, "The eigentrust algorithm for reputation management in p2p networks.," in *12th International Conference on World Wide Web,* Budapest, 2003, pp. 640–651.

[123] A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support System,* vol. 43, pp. 618–644, 2007.

[124] A. Josang and J. Golbeck, "Challenges for robust trust and reputation systems," in *International Workshop on Security and Trust Management (STM),* SaintMalo, France, 2009.

[125] C. Dellarocas, "Reputation mechanism design in online trading environments with pure moral hazard," *Information Systems Research,* vol. 16, pp. 209-230, 2005.

[126] N. Tyagi and S. Simple, "Weighted page rank algorithm based on number of visits of links of web page," *International Journal of Soft Computing and Engineering (IJSCE),* pp. 2231-2307., 2012.

[127] Y. Ding, "Topic-based PageRank on author cocitation networks," *Journal of the Association for Information Science and Technology,* vol. 62, pp. 449-466, 2011.

[128] L. Backstrom and L. Jure, "Supervised random walks: predicting and recommending links in social networks," in *The fourth ACM international conference on Web search and data mining,* HongKong, 2011, pp. 635-644.

[129] M. Franceschet, "PageRank: Standing on the shoulders of giants," *Communications of the ACM,* vol. 54, pp. 92-101, 2011.

[130] Y. Ren and A. Boukerche, "Modeling and managing the trust for wireless and mobile ad hoc networks," in *IEEE International Conference on Communication (ICC'08),* Beijing, China, 2008, pp. 2129-2133.

[131] R. A. Shaikh, H. Jameel, S. Lee, Y. J. Song, and S. Rajput, "Trust management problem in distributed wireless sensor networks," in *IEEE international conference on Embedded and real-time computing systems and applications*, New South Wales, Australia, 2006, pp. 411-414.

[132] F. Bao, R.Chen, and J. Guo, "Scalable, adaptive and survivable trust management for community of interest based internet of things systems," in *IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)*, Mexico City, Mexico, 2013.

[133] S. Buchegger and L. B. Jean-Yves, "A robust reputation system for peer-to-peer and mobile ad-hoc networks," in *P2P Econ*, Berkeley, U.S, 2004.

[134] U. Jayasinghe, H. W. Lee, and G. M. Lee, "A computational model to evaluate honesty in social Internet of things," in *The 32nd ACM Symposium on Applied Computing*, Marrakesh, Morocco, April, 2017.

[135] N. B. Truong, T. U. Won, and G. M. Lee, "A Reputation and Knowledge Based Trust Service Platform for Trustworthy Social Internet of Things," in *Innovations in Clouds, Internet and Networks (ICIN)*, Paris, France, 2016.

[136] E. Chang, F. K. Hussain, and T. S. Dillon, "Fuzzy nature of trust and dynamic trust modeling in service oriented environments," in *The 2005 workshop on Secure web services*, Fairfax, USA, 2005.

[137] W. Z. Khan, Y. Xiang, M. Y. Aalsalem, and Q. Arshad, "Mobile phone sensing systems: A survey," *IEEE Communications Surveys & Tutorials,* vol. 1, pp. 402-427, 2013.

[138] R. K. Ganti, F. Ye, and H. Lei, "Mobile crowdsensing: current state and future challenges," *IEEE Communications Magazine,* vol. 11, 2011.

[139] B. Guo, C. Chen, D. Zhang, Z. Yu, and A. Chin, "Mobile crowd sensing and computing: when participatory sensing meets participatory social media," *IEEE Communications Magazine,* vol. 54, pp. 131-137, 2016.

[140] G. Ding, J. Wang, Q. Wu, L. Zhang, Y. Zou, Y. D. Yao*, et al.*, "Robust spectrum sensing with crowd sensors.," *IEEE Transactions on Communications,* vol. 62, pp. 129-3143, 2014.

[141] J. Liu and W. Sun, "Smart Attacks against Intelligent Wearables in People-Centric Internet of Things," *IEEE Communications Magazine,* vol. 54, pp. 44-49, 2016.

[142] J. Gubbia, R. Buyyab, M. Palaniswami, and S. Marusic, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems,* vol. 29, pp. 1645–1660, 2013.

[143] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi*, et al.*, "Internet of things strategic research roadmap," *Internet of Things-Global Technological and Societal Trends,* pp. 9-52, 2011.

[144] J. S. Silva, P. Zhang, T. Pering, F. Boavida, T. Hara, and N. C. Liebau, "People-Centric Internet of Things," *IEEE Communications Magazine,* vol. 55, pp. 18-19, 2017.

[145] B. Guo, Z. Yu, X. Zhou, and D. Zhang, "From participatory sensing to mobile crowd sensing," in *IEEE International Conference on Pervasive Computing and Communication Workshops (PERCOM WORKSHOPS)*, Budapest, 2014, pp. 593-598.

[146] F. Delmastro, V. Arnaboldi, and M. Conti, "People-centric computing and communications in smart cities," *IEEE Communications Magazine,* vol. 54, pp. 122-128, 2016.

[147] A. Capponi, C. Fiandrino, D. Kliazovich, P. Bouvry, and S. Giordano, "A Cost-Effective Distributed Framework for Data Collection in Cloud-based Mobile Crowd Sensing Architectures," *IEEE Transactions on Sustainable Computing,* vol. 2, pp. 3-16, 2017.

[148] M. R. Ra, B. Liu, T. F. LaPorta, and R. Govindan, "Medusa: A programming framework for crowd-sensing applications," in *10th international conference on Mobile systems, applications, and services*, United Kingdom, June, 2012, pp. 337-350.

[149] D. Zhang, L. Wang, H. Xiong, and B. Guo, "4W1H in mobile crowd sensing," *IEEE Communications Magazine,* vol. 52, pp. 42-48, 2014.

[150] S. Reddy, D. Estrin, and M. Srivastava, "Recruitment framework for participatory sensing data collections," in *International Conference on Pervasive Computing*, Finland, May, 2010, pp. 138-155.

[151] M. Karaliopoulos, O. Telelis, and I. Koutsopoulos, "User recruitment for mobile crowdsensing over opportunistic networks," in *IEEE Conference on Computer Communications (INFOCOM)*, HongKong, April, 2015, pp. 2254-2262.

[152] D. Zhang, H. Xiong, L. Wang, and G. Chen, "CrowdRecruiter: selecting participants for piggyback crowdsensing under probabilistic coverage constraint," in *ACM International Joint Conference on Pervasive and Ubiquitous Computing*, Seattle, USA, September, 2014, pp. 703-714.

[153] N. D. Lane, Y. Chon, L. Zhou, Y. Zhang, F. Li, D. Kim*, et al.*, "Piggyback CrowdSensing (PCS): energy efficient crowdsourcing of mobile sensor data by exploiting smartphone app opportunities," in *11th ACM Conference on Embedded Networked Sensor Systems*, Roma, Italy, November, 2013.

[154] C. H. Liu, B. Zhang, X. Su, J. Ma, W. Wang, and K. K. Leung, "Energy-aware participant selection for smartphone-enabled mobile crowd sensing," *IEEE Systems Journal*, vol. 11, pp. 1435-1446, 2017.

[155] S. He, D. H. Shin, J. Zhang, and J. Chen, "Toward optimal allocation of location dependent tasks in crowdsensing," in *INFOCOM*, Toronto, Canada, April, 2014, pp. 745-753.

[156] C. Fiandrino, B. Kantarci, F. Anjomshoa, D. Kliazovich, P. Bouvry, and J. Matthews, "Sociability-driven user recruitment in mobile crowdsensing internet of things platforms," in *Global Communications Conference (GLOBECOM)*, Washington DC, U.S, December, 2016.

[157] D. Yang, G. Xue, X. Fang, and J. Tang, "Crowdsourcing to smartphones: Incentive mechanism design for mobile phone sensing," in *International conference on Mobile computing and networking (Mobicom)*, Istanbul, Turkey, August, 2012, pp. 173-184.

[158] B. Kantarci and H. T. Mouftah, "Trustworthy sensing for public safety in cloud-centric internet of things," *IEEE Internet of Things Journal*, vol. 1, pp. 360-368, 2014.

[159] B. Kantarci, K. G. Carr, and C. D. Pearsall, "SONATA: Social Network Assisted Trustworthiness," *Int'l J. Distributed Systems,* vol. 7, pp. 64–84, 2016.

[160] M. Pouryazdan and B. Kantarci, "The smart citizen factor in trustworthy smart city crowdsensing," *IT Professional*, vol. 18, pp. 26-33, 2016.

[161] B. Kantarci and H. T. Mouftah, "Trustworthy crowdsourcing via mobile social networks," in *Global Communications Conference (GLOBECOM)*, Austin, TX, USA, December, 2014, pp. 2905-2910.

[162] J. An, X. Gui, Z. Wang, J. Yang, and X. He, "A crowdsourcing assignment model based on mobile crowd sensing in the internet of things," *IEEE Internet of Things Journal*, vol. 2, pp. 358-369, 2015.

[163] R. Bhoraskar, N. Vankadhara, B. Raman, and P. Kulkarni, "Wolverine: Traffic and road condition estimation using smartphone sensors," in *International Conference on Communication Systems and Networks (COMSNETS)*, Bangalore, India 2012.

[164] P. Mohan, V. N. Padmanabhan, and R. Ramjee, "Nericell: rich monitoring of road and traffic conditions using mobile smartphones," in *ACM conference on Embedded network sensor systems*, Raleigh, NC, USA, 2008, pp. 323-336.

[165] L. MovableType, "Calculate distance, bearing and more between Latitude/Longitude points," ed: Movable Type Ltd., 2016.

[166] F. Anjomshoa, M. Catalfamo, D. Hecker, N. Helgeland, and A. Rasch, "Sociability assessment and identification of smartphone users via behaviormetric software," in *IEEE Symposium on Computers and Communications (ISCC)*, Messina, Italy, June 2016.

[167] C. Fiandrino, B. Kantarci, F. Anjomshoa, D. Kliazovich, P. Bouvry, and J. Matthews, "Sociability-Driven user recruitment in mobile crowdsensing Internet of Things Platforms," in *IEEE Global Communications Conference (GLOBECOM)*, Washington DC, USA, 2016.

[168] N. B. Truong, T. W. Um, B. Zhou, and G. M. Lee, "From personal experience to global reputation for trust evaluation in the social internet of things," in *IEEE Global Communications Conference (GLOBECOM)*, Singapore, 2017.

[169] P. Y. Chen, S. M. Cheng, P. S. Ting, C. W. Lien, and F. J. Chu, "When Crowdsourcing Meets Mobile Sensing: A Social Network Perspective," *IEEE Communications Magazine,* vol. 53, pp. 157-163, 2015.

[170] J. Weppner, P. Lukowicz, U. Blanke, and G. Tröster, "Participatory Bluetooth scans serving as urban crowd probes," *IEEE Sensors Journal*, vol. 14, pp. 4196-4206, 2014.

[171] R. Zhang, J. Zhang, Y. Zhang, J. Sun, and G. Yan, "Privacy-preserving profile matching for proximity-based mobile social networking," *IEEE Journal on Selected Areas in Communications*, vol. 31, pp. 656-668, 2013.

[172] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Sensing as a service model for smart cities supported by internet of things," *Transactions on Emerging Telecommunications Technologies*, vol. 25, pp. 81-93, 2014.

[173] G. Merlino, S. Arkoulis, S. Distefano, C. Papagianni, A. Puliafito, and S. Papavassiliou, "Mobile crowdsensing as a service: a platform for applications on top of sensing clouds," *Future Generation Computer Systems*, vol. 56, pp. 623-639, 2016.

[174] D. Christin, "Privacy in mobile participatory sensing: Current trends and future challenges," *The Journal of Systems and Software*, vol. 116, pp. 57-68, June 2016.

[175] N. Laranjeiro, S. N. Soydemir, and J. Bernardino, "A Survey on Data Quality: Classifying Poor Data," in *21st Pacific Rim International Symposium on Dependable Computing*, Zhangjiajie, 2015.

[176] N. Askham, D. Cook, M. Doyle, H. Fereday, M. Gibson, U. Landbeck, *et al.*, "The six primary dimensions for data quality assessment," DAMA UK Working Group, United Kingdom2013.

[177] N. Laranjeiro, S. N. Soydemir, and J. Bernardino, "A survey on data quality: classifying poor data," in *IEEE 21st Pacific Rim International Symposium on Dependable Computing (PRDC)*, Melbourne, Australia, 2015.

[178] D. Loshin, *The Practitioner's Guide to Data Quality Improvement* vol. A volume in MK Series on Business Intelligence. Boston: Elsevier, 2011.

[179] L. Pipino, W. Lee, and R. Wang, "Data quality assessment," *Communications of the ACM*, vol. 45, pp. 211-218, 2002.

[180] H. Kim, A. Ahmad, J. Hwang, H. Baqa, F. LeGall, M. A. R. Ortega, *et al.*, "IoT-TaaS: Towards a Prospective IoT Testing Framework," *IEEE Access*, 2018.

[181] C. Dellarocas, "The digitization of word of mouth: Promise and challenges of online feedback mechanisms," *Management science*, vol. 49, pp. 1407-1424, 2003.

[182] S. Geisser, *Predictive Inference: An Introduction*. Great Britain: Chapman & Hall, 2017.

[183] C. Batini and M. Scannapieco, *Data Quality: Concepts, Methodologies and Techniques*: Springer Berlin Heidelberg, 2006.

[184] T. C. Redman, "The impact of poor data quality on the typical enterprise," *Communications of the ACM*, vol. 41, pp. 79-82, 1998.

[185] G. White, V. Nallur, and S. Clarke, "Quality of service approaches in IoT: A systematic mapping," *Journal of Systems and Software*, vol. 132, pp. 186-203, 2017.

[186] N. Truong, T. W. Um, B. Zhou, and G. M. Lee, "Strengthening the Blockchain-based Internet of Value with Trust," in *IEEE International Conference on Communications (ICC)*, Kansas, U.S.A, 2018.

[187] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based Framework for High Integrity Sensor Networks," *ACM Transactions on Sensor Networks*, vol. 5, 2007.

[188] P. N. Mahalle, P. A. Thakre, N. R. Prasad, and P. Prasad, "A fuzzy approach to trust based access control in internet of things," in *IEEE Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE)*, Atlanta, USA, 2013.

[189] I. Chen, F. Bao, and J. Guo, "Trust-based Service Management for Social Internet of Things Systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, pp. 684-696, 2016.

[190] E. Jacquet-Lagrèze, Siskos, J., "C," *European Journal of Operational Research*, pp. 151-164, 1982.

[191] Q. H. Cao, G. Madhusudan, R. Farahbakhsh, and N. Crespi, "Usage Control for Data Handling in Smart Cities," in *IEEE Global Communications Conference (GLOBECOM)*, San Diego, CA, 2015.

[192] Q. H. Cao, I. Khan, R. Farahbakhsh, G. Madhusudan, G. M. Lee, and N. Crespi, "A Trust Model for Data Sharing in Smart Cities," in *IEEE International Conference on Communications (ICC 2016)*, Kuala Lumpur, Malaysia, 2016.

[193] J. Park and R. Sandhu, "Towards usage control models: Beyond Traditional Access Control," in *Seventh ACM Symposium on Access Control Models and Technologies*, New York, USA, 2002.

[194] J. Park and R. Sandhu, "The UCON ABC Usage Control Model," *ACM Transactions on Information and System Security (TISSEC)*, vol. 7, pp. 128-174 2004

[195] A. Lazouski, Martinelli, F., Mori, P., "Usage control in computer security: A survey," *Computer Science Review*, vol. 4, pp. 81-99, 2010.

[196] J. Pato, Paradesi, S., Jacobi, I., Shih, F., Wang, S., "Aintno: Demonstration of Information Accountability on the Web," in *IEEE Third International Conference on Privacy, Security, Risk and Trust (PASSAT)*, Boston, MA, 2011.

[197] S. Speiser, Wagner, A., Raabe, O., Harth, A., "Web Technologies and Privacy Policies for the Smart Grid," in *Annual Conference of the IEEE Industrial Electronics Society (IECON 2013)*, Vienna, Austria, 2013.

[198] I. Khan, F. Belqasmi, R. Glitho, N. Crespi, M. Morrow, and P. Polakos, "Wireless sensor network virtualization: early architecture and research perspectives," *IEEE Network*, vol. 29, pp. 104-112, June 2015.

[199] I. Khan, R. Jafrin, F. Errounda, R. Glitho, N. Crespi, M. Morrow, *et al.*, "A data annotation architecture for semantic applications in virtualized wireless sensor networks," in *IFIP/IEEE International Symposium on Integrated Network Management (IM 2015)*, Ottawa Canada, May 2015.

[200] M. Compton, Barnaghi, P., Bermudez, L., GarcíA-Castro, R., Corcho, O., Cox, S., Huang, V. , "C," *Web Semantics: Science, Services and Agents on the World Wide Web*, vol. 17, pp. 25-32, 2012.

[201] D. Nute, *Defeasible logic: Handbook of Logic in Artificial Intelligence and Logic Programming*. New York, USA: Oxford University Press, 1994.

[202] E. Kontopoulos, Bassiliades, N., Governatori, G., Antoniou, G., "A modal defeasible reasoner of deontic logic for the semantic web," *International Journal on Semantic Web and Information Systems (IJSWIS)*, vol. 7, pp. 18-43, 2011.

[203] G. Antoniou, Dimaresis, N., Governatori, G., "A modal and deontic defeasible reasoning system for modelling policies and multi-agent system," *Expert Systems with Applications*, vol. 36, pp. 4125–4134, 2009.

[204] D. Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," Cisco White Paper2011.

[205] J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin, *et al.*, "Unlocking the potential of the Internet of Things," McKinsey Global Institute (MGI)2015.

[206] D. O'mahony, M. Peirce, and H. Tewari, *Electronic payment systems*. Norwood: Artech House, 1997.

[207] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[208] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*: Princeton University Press, 2016.

[209] R. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, technology, and governance," *The Journal of Economic Perspectives*, vol. 29, pp. 213-238, 2015.

[210] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in Bitcoin," in *ACM conference on Computer and communications security*, NC, USA, 2012, pp. 906-917.

[211] B. Jerry and A. Castillo, *Bitcoin: A primer for policymakers.*: Mercatus Center at George Mason University, 2013.

[212] V. Buterin, "White Paper: A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum Company2014.

[213] R. C. Merkle, "Protocols for public key cryptosystems," in *IEEE Symposium on Security and Privacy*, 1980, pp. 122-134.

[214] I. Eyal, A. E. Gencer, E. G. Sirer, and R. V. Renesse, "Bitcoin-NG: a scalable blockchain protocol," in *Usenix Conference on Networked Systems Design and Implementation (NSDI'16)*, CA, U.S, 2016, pp. 45-59.

[215] M. Iansiti and K. R. Lakhani, "The Truth About Blockchain," *Harvard Business Review*, vol. 95, pp. 118-127, 2017.

[216] M. Swan, *Blockchain: Blueprint for a new economy*: O'Reilly Media, Inc., 2015.

[217] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *IEEE Symposium on Security and Privacy (SP)*, CA, U.S, 2016, pp. 839-858.

[218] L. L. Pipino, Y. W. Lee, and R. Y. Wang, "Data quality assessment," *Communications of the ACM*, vol. 4, pp. 211-218, 2012.

[219] "Web Hosting Service," ed: Wikipedia, 2016.