Marie Skłodowska-Curie Actions (MSCA)

Research and Innovation Staff Exchange (RISE)

H2020-MSCA-RISE-2017

Intelligence-Driven Urban Internet-of-Things Ecosystems for Circular, SAfe and IncLusive Smart CITIES

D2.2: Risk Analysis, User, Trust and Reputation models for Smart Cities

Abstract: This deliverable focuses on the analysis of the model for quantifying the security and economic risk perceived by user models defining the methodology for identifying security properties that improves the security perception of a given persona.

Contractual Date of Delivery	31/12/2019
Actual Date of Delivery	31/12/2019
Deliverable Security Class	Public
Editor	Cablenet
Contributors	All Partners

The *IDEAL-CITIES* consortium consists of:

FOUNDATION FOR RESEARCH AND TECHNOLOGY -HELLAS	FORTH	GR
ECOLE NATIONALE DES PONTS ET CHAUSSEES	ENPC	FR
BOURNEMOUTH UNIVERSITY	BU	UK
BLUESOFT SPOLKA Z OGRANICZONA ODPOWIEDZIALNOSCIA	BLS	PL
CABLENET COMMUNICATION SYSTEMS LTD	CBN	CY
NODAL POINT SYSTEMS	NPS	GR

This project is supported by the European Commission under the Horizon 2020 Program (2014-2020) with Grant agreement no: 778229

Document Revisions & Quality Assurance

Internal Reviewers

1. Andreas Miaoudakis, FORTH
2. Jakub Rola, BLS
3. Amalia Diamianou, BU
4. Vlatka Katusic Cuentas, ENPC
5. Kyriaki Konstantinou, CBN

Revisions

Version	Date	By	Overview
1.0	20/05/19	Kyriaki Konstantinou (Cablenet)	ToC defined
1.1	28/05/19	Kyriaki Konstantinou (Cablenet)	ToC assignment
1.2	20/06/19	Andreas Miaoudakis (FORTH)	Section Contribution
1.3	01/07/19	Amalia Diamianou (BU)	Section Contribution
1.3	28/6/19	Andreas Miaoudakis and Georgia Koutsouri, FORTH	Review and Finalize of first draft
1.4	1/11/19	Kyriaki Konstantinou (Cablenet)	Consolidation and address comments
1.5	13/11/19	Kyriaki Konstantinou (Cablenet)	Conclusion draft Update of ToC according to the last regular telco
1.6	27/11/19	Kyriaki Konstantinou (Cablenet)	Consolidation (Final Draft)
1.7	04/12/19	Vlatka Katusic Cuentas (ENPC)	Section Contribution
1.71	04/12/19	Kyriaki Konstantinou (Cablenet)	ENPC feedback review and consolidation
1.72	10/12/19	Andreas Miaoudakis (FORTH)	Review of sections 1, 2.2.4 and 5
1.73	16/12/19	Amalia Diamianou (BU)	Review of sections 2.1, 2.2.2 and 3.2
1.8	18/12/19	Kyriaki Konstantinou (Cablenet)	Consolidate feedbacks and second draft
1.81	20/12/19	Kyriaki Konstantinou (Cablenet)	Referencing review and finalization
1.91	20/12/19	Jakub Rola (BLS)	Review of sections 2.2, 2.2.1 and 3.1.1
2.00	20/12/19	Kyriaki Konstantinou (Cablenet)	Consolidation and finalization

Table of Contents

1 Introduction

The use of Internet of Things (IoT) have increased a lot in recent years. IoT have been adopted in various economic sectors, which include health, manufacturing and recently development of smart cities [1]. Despite the increased adoption of IoT in the world, IoT does not operate in isolation but rather relies on other technologies to flourish. This means that the IoT infrastructure comprises of billions of interconnected devices and sensors. The sensors help to monitor different human aspects and transmit information to the connected devices. Research indicates that by the year 2020, over billion devices will be connected to the internet. This means that the amount of data transactions will grow 10-fold within the next years [2].

IoT brings new possibilities and transforms the functionalities of Wireless Sensor Networks (WSNs) and Mobile networks. The connection of sensors and devices to the internet has facilitated transmission of data of various applications that include smart city, e-health, smart transportations and smart homes among others [3]. The internet connection helps IoT to bridge the gap between the physical and the virtual world. The IoT paradigm makes it possible for devices and sensors to be connected to the internet. This makes it possible for the devices and sensors to be controlled form a remote location.

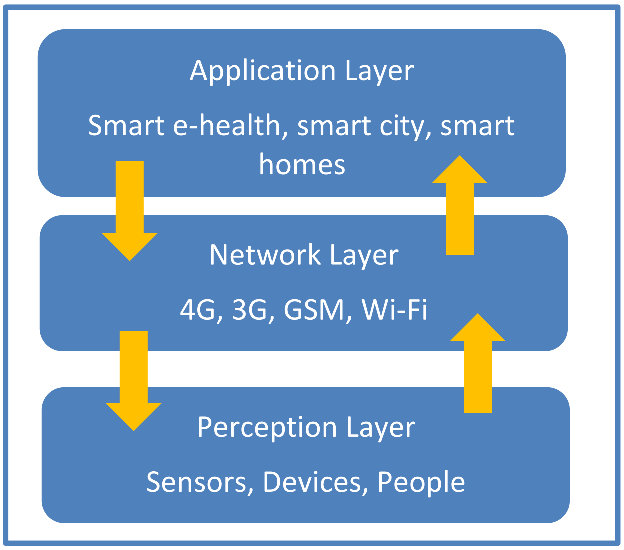

Figure 1: Smart Cities data flow

To facilitate efficient communication and interaction among devices, sensors and human beings, an IoT architecture/framework is required. Typically an IoT architecture consists of three layers; the network layer, the application layer and the perception layer. The perception layer deals with the physical things in IoT ecosystem [1]. This layer is the lowest layer and comprises of the people, devices and sensors. The perception layer collects data through sensing and sends that data to the upper layer; network layer. The network layer transmits the received data from the perception layer over various network layer technologies. Such technologies include ad-hoc network elements like the Bluetooth, Wireless Fidelity (Wi-Fi) and Zigbee [4]. The network layer further contains broader network infrastructure that include mobile networks among others (GSM, 3G, LTE etc.). The network elements forward the received data to the application layer to be acted upon. Figure 1 depict the described data flow. For example, if the perception layer sensors indicate low temperatures, the network layer transmits the data to the application layer. The application layer will act on the data, convert it to meaningful information and trigger the heater to be turned on in case of a smart home environment.

Smart transport systems is another area that has benefited from IoT [5], [6]. In smart transportation, smart cars are fitted with internet connections where the cars can communicate with weather forecast stations and this can help in case of bad weather. Current vehicle models are fitted with sensors that can sense vehicles at certain proximities and trigger emergency breaking systems. Vehicles are also fitted with Global Positioning System (GPS) that help to receive data regarding traffic jams and other incident information [5].

Despite the immense benefits brought about by IoT, various issues like privacy, security and trust continue to affect the full realization and adoption of the IoT objectives [6] [7]. Security in crucial is IoT since it guarantees that data collected from people, devices and sensors is not tampered with and reaches the network layer as it is. Privacy in IoT helps to assure the parties to a smart network; for example, a smart home that the IoT systems is secure and no third party can access the data collected or can interfere with the signals triggered by the application layer. Trust is collated to privacy and it involves various devices or sensors developing the same trust level like normal human beings.

2 Background

IoT involves collection and aggregation of data from various physical environments. Due to the variety and differences in these environments, some difficulties arise like data management risks and discrimination brought about by aggregation and analytic of the gathered personal sensitive data that may include names, contacts and locations among others [5]. Due to these issues, trust can be used to enhance interaction between the humans and services to help reduce risks when making crucial decisions and overcome uncertainty. Therefore, introducing a trust platform can assist in reducing the unforeseen risks and enhance predictability.

2.1 Trust

Trust is described as a 'belief' of the trusting party (trustor) in the party being trusted (trustee) that a particular task will be carried out as agreed between the two parties [8]. This implies that the trustor identifies a potential risk when dealing with the trustee. At the same time, trustors must bring themselves at a vulnerable level ready to be compromised by depending on the trustee since there is no guarantee that the trustee will meet the set conditions [9].

Trust is a diverse concept used in various disciplines like computer science, psychology and human society among other disciplines. Researchers observe that when a human being believes in another human being, that belief not only relies on the trustee's character and trustor's perception of the trustee but also depends on time and surroundings [8]. Various trust models have been developed but very few can be adopted in the field of computer science [9]. However, trust is a basic human aspect when it comes to interactions of an occasion like the communication of person, or things communicating with people or react to each other. As an extent this makes it crucial when evaluating interaction between various IoT elements.

Evaluation of trust requires analysis of the trustor's perception of the trustee, the trustee's character and the environmental influences. These factors can be described as trustor's "propensity, trustee's trustworthiness and environmental risks" [8]. A major point to note is that trust cannot be viewed as a trustor's property nor is a trustee's property but it is an interrelation between the relationship that exists between the trustor and trustee.

Definition of trust is very important as it gives the foundation unto which a trust model that can accommodate even the needs of special people in smart cities, like the sensitive groups such as elderlies, kinds, pregnant women, people with hearing loss, disabled people and so on Understanding the basis of how trust works makes it vital in generating ideas and integrating the current trust models to make them incorporate special people living in smart cities.

2.2 Citizen Centric - Smart Cities

In the last few years, various major cities that include New York, Singapore, Cairo, Tokyo and Seoul among others have embarked on making their cities smart [1], [9]. Initially, smart cities have been referred as the cities of the future but due to the recent technological advancements and information flow, it is evident that majority of the upcoming cities will adopt the smart city model.

A smart city can be defined as "a city that strategically utilizes many smart factors such as Information and Communication Technology to increase the city's sustainable growth and strengthen city functions, while guaranteeing citizens' happiness and wellness. [9]" Smart cities require proper planning during the initial stages. This means that a smart city will be well defined based on the cities objectives set by all the stakeholders. The initial smart cities approaches mostly concentrated on incorporating technologies in the cities to accelerate service delivery and human development [10]. However, the original urban designers and architects forgot an important component during their design; the human factor. Human involvement during the design and development of a smart city means that the needs of people come first. The Human-Centric Smart City concept proposes to develop a citizen-driven, smart, all-inclusive and sustainable environment, with a new governance framework in which citizens and government engage in exchanging their opinions in the decision procedures for the City. This way a smart city being is defined by its inhabitants' needs and demands.

As smart cities are expected to be an integral part of citizens' life, it is then essential to include their views in its design. Participatory Design [11] approach seems to be a sensible choice both to incorporate the views of citizen's actively through co-designing with them for services and infrastructure and also to give a sense of ownership and responsibility so that application of smart city model is increased. The challenges would be that smart cities are systems of systems [12] and users, without the right support with techniques like reduction and simulation, may provide partial and inaccurate views. Hence, the use of advanced techniques like virtual reality and creative design combined with daily life data captured on the move would be a good approach [13].

With smart cities, and due to the dynamic nature of their interactions and the emergence of new services and areas, one would expect smart cities design to evolve. Evolution by design means that cities are planned to change in an agile style where infrastructure allows for expansion and replacement without disruption of services. One essential element in that is citizens themselves. The concept of Social Sensing [14] denotes the role of people in providing information, which enables the planning of systems evolutions. Figure 2 shows the high-level picture of such citizen engagement. In self-adaptive systems, the monitoring part is the first step where the other steps are analysis, planning and implementation, i.e. the MAPE loop [14] [15]. Hence, autonomic computing and autonomous systems [16] can both benefit from users acting as sensors and providing feedback and increase acceptance and adoption by doing so as citizens are given right in the decision making the process through voting and reporting issues.

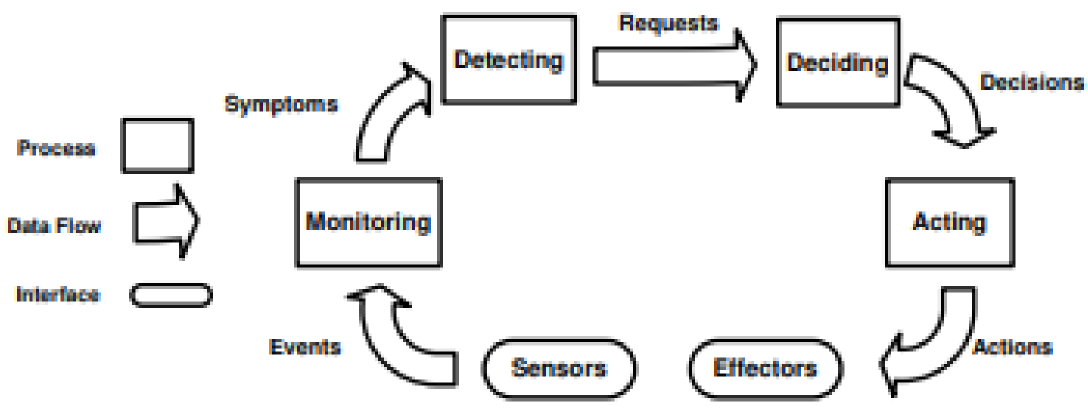

Figure 2 Four Adaptation Processes in Self- Adaptive Software [15]

Besides the reliance on people to provide feedback on the quality of certain design strategy and the context in which they prove to be successful or limited, the expectation of a user-centric smart city is to reflect and respond to that feedback. The notion of Social Adaptation [17] is the democratic process of allowing people to take an active role in shaping future systems decisions. This is related to the concept of Wisdom of the Crowd [18] where the fundamental argument is that the right selection and aggregation of the opinions of a large number of ordinary people can be better than relying on elite experts. However, the challenge is to get that right selection and aggregations. Guidelines and principles are given to reach that aim and this includes diversity in the crowd, decentralisation where each group provide feedback on their relevant area of knowledge, independence where there is no felt and seen hierarchy and suppression, etc.

Central to the inclusion of citizens in the decision-making process is to motivate them to take that role. Motivating citizens can be done through the design of the city itself, e.g. by involving gamification and persuasive technology techniques [19]. For example, techniques like social recognition can be used to give credit to citizens who detect more faults and where these faults are seen to be significant and relevant to other citizens. Rewarding can be although through the so-called infotainment, i.e. information and entertainment. For example, upon providing a certain service, e.g. using augmented reality for touristic explanation, the system can show how this compares to other volunteers design and how certain demographics rate the design and how they see it.

Citizens are diverse in their preferences towards such motivational techniques, and their engagement in the design and decision-making process can prove to be difficult with personalising that engagement process [20]. According to [21], a user-centric design of feedback-based approaches can take into account five main personas:

- *Privacy-tolerant and socially* ostentatious crowd members expect acknowledgement in return for their feedback.
- *Privacy-fanatical but generous* crowd members are motivated by respect for privacy.
- Passive and stingy crowd members are motivated by seeing others' feedback and contributing minimally.
- *Loyal and passionate* crowd members care about the software's sustainability and reputation but give less objective feedback.
- *Incentive seekers* care about monetary incentives and pay limited attention to feedback quality.
- *Perfectionists and complainers* are motivated by the self-satisfaction achieved after discovering and flagging a problem.
- *Impact seekers* are motivated by seeing their suggested changes implemented.

Another dimension of user-centric design is to explain the decisions taken within the smart city design to citizens in a way that is personalised and easy to follow. A review of the literature shows us that such explanation and personalisation is likely to increase adoption and at the same time increase liability. Figure 3 shows the number of papers in personalising explanation of smart and intelligent systems. The needs category denote papers which addressed the motivations to personalise explanation and the Implementation category shows the number of papers which tackled ways to implement the personalisation.

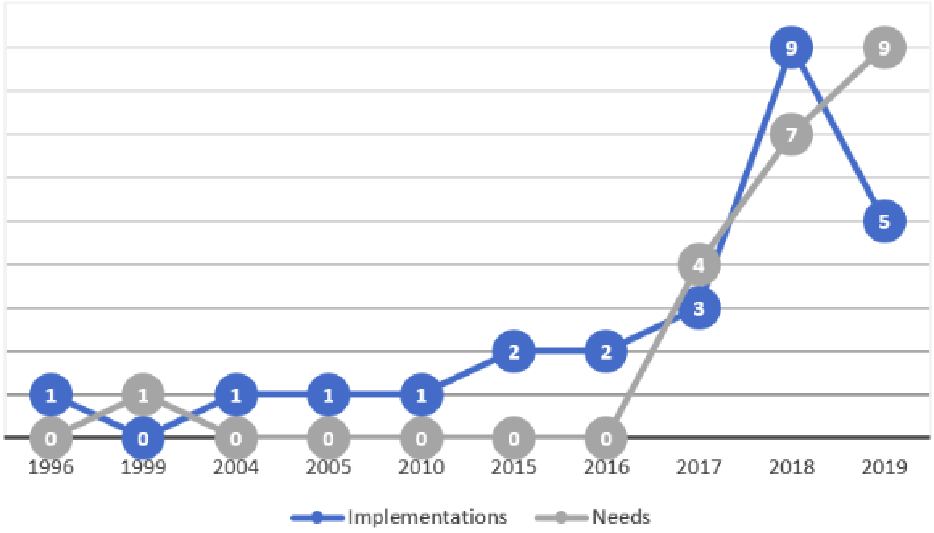

Figure 3 Research papers about personalising explanation

In summary, the personalisation follows different techniques such as user modelling and profiling [22], users goals and intentions [23], dialogue with users [24] [25], ratings and reviews by the user [26] and collaborative filtering [27] [28]. While these approaches are meant for systems with direct interaction with users, e.g. e-commerce and health, the challenge is higher since cognitive load and distractions are factors considered Evolution of Smart Cities

The concept of making urban centres become sustainable for development has been there since ancient times. Ebenezer Howard; a British urban planner, published a book "*Garden Cities of To-morrow*" in 1998 discussed 'urbanism' as a way of changing the slums into neighbourhoods that can support employment opportunities and provide comfort to its dwellers [9]. The concept of smart city has evolved over time. The section below discusses the various names of smart cities over the years;

a. Sustainable city - the concept of sustainable city was coined in the United Nations Brundtland Commission report of 1987 [2]. This term focused on making urban centres sustainable for development and gave the various strategies that cities should adopt to control climate change.
b. Digital cities – this concept was documented by the European Commission in its programme 'European Digital Cities' between 1996 and 1999 [9]. This concept sought to incorporate the technological evolution in supporting complex city environments through developing digital networks and informative programs. The program also focused on providing the local communities with the relevant services and involving them in city decision making programs.
c. Smart cities – this concept incorporates various elements that include sustainability, internet technologies and social inclusion.
d. Future of cities – this concept incorporates peoples' aspirations, vision and goals and how they would like their cities to operate. Future cities defines how people, business, authorities and environment will interact. This is also referred to as human-centric cities.

2.2.1 Characteristics of Smart Cities

A smart city is described by the physical and legislation infrastructures that support the various activates that include economic development, facilitate social inclusion and safeguarding of environment.

One of the characteristic, of smart city is the infrastructure development. The infrastructure development not only seeks to improve and establish the communication channels of the services provided to the users but also allows its constant alignment with the continual improvement and development of the technology's future growth. Examples of the services supported by the communicated channels of the infrastructure development is housing services, telecommunication services and so on.

Another characteristic of the smart city is the enhancement of any new socio-economic development within the smart city system, allowing the expansion of urban sectors and creating a competitive environment, as an ultimate strategy [29]. This will allow a sustainable development and growth of the smart city providing new opportunities for continual improvement to more sectors, such as the energy management, the environment protection through the preservation of natural resources and so on [29].

From the Quality perspective, the Standard 37120/2014 (*Sustainable development of communities*) defines 17 key necessities for a successful smart city. These indicators include *economy, education, energy, environment, finance, fire and emergency responses, governance, health, recreation, safety, shelter, solid waste, telecommunications and innovations, transportation, urban planning, water and sanitation.*

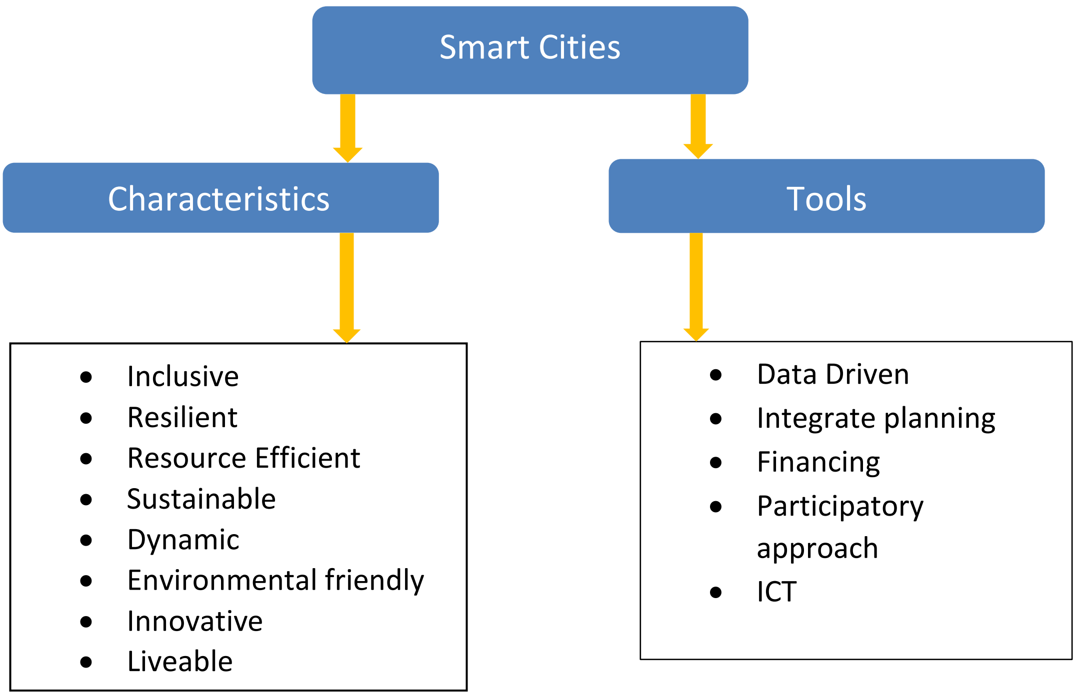

Figure 4: Smart Cities Characteristics

The other standard [30] - ISO/TS 37151:2015 - gives principles and specifies requirements for the *definition*, *identification*, *optimization*, and *harmonization* of community infrastructure performance metrics, and gives recommendations for analysis, including *smartness*, *interoperability*, *synergy*, *resilience*, *safety*, and *security* of community infrastructures. The standard ISO/TS 37151:2015 recognizes that community infrastructures include, but are not limited to, *energy*, *water*, *transportation*, *waste*, and *ICT*. The selection and the importance of metrics or key performance indicators of community infrastructures is a result of the application of this standard and depends on the characteristics of each community. This standard defines *smart community infrastructure* as “community infrastructure with enhanced technological performance that is designed, operated, and maintained to contribute to sustainable development and resilience of the community”. The *sustainability development* characteristics means “state of the global system, including environmental, social and economic aspects, in which the needs of the present are met without compromising the ability of future generations to meet their own needs”.

The UNE 178301:2015 Spanish standard [31] establishes the specific set of guidelines in the form of requirements, techniques, common vocabularies and indicators for the reuse of documents and information resources produced or held by the public sector when it comes terming Open Data or Open Data, in the field of Smart Cities.

2.2.2 Related Standards for smart cities:

- ISO/WD 37120 Sustainable development of communities -- Indicators for city services and quality of life
- ISO/NP 37122 Sustainable development in communities -- Indicators for Smart Cities
- ISO/DTR 37121 Inventory and review of existing indicators on sustainable development and resilience in cities
- ISO/DIS 37101 Sustainable development of communities -- Management systems -- Requirements with guidance for resilience and smartness
- ISO 37120:2014 2014 - Sustainable development of communities -- Indicators for city services and quality of life
- UNE 178301:2015 2015 - Smart Cities. Open Data.
- ISO/TS 37151:2015 2015 - Smart community infrastructures -- Principles and requirements for performance metrics.
- Smart cities’ ICT Infrastructure

The core infrastructure of a smart city is the Information and communication Technology (ICT) [32]. ICT facilitates communication between network layer elements and transmission of real-time data from the perception layer. It further helps to transmit triggers from the application layers to the IoT devices. Various city functions and services hugely depend on the ICT infrastructure and these reliance results to a convergence of activities that facilitate the smooth running of a smart city as a big, independent intelligence unit [32]. In terms of structures, a smart city comprises of many systems. The independent systems and individuals come together to form the meta-systems. These meta-systems then combine to form sub-systems. Proper functioning of these independent sub-systems and systems requires openness and the industrial standards to be adhered to. Lack of openness and standardization in a smart city leads to reduce scope and increased cost of construction of the smart city consecutively.

The main difference between a smart city and a traditional city is that a smart city uses a service-driven ICT infrastructure to establish a relationship with its citizens. Although the traditional cities have ICT supported infrastructures, these infrastructures are not flexible and cannot respond to changing societal contexts like economy and culture [9]. Smart cities are flexible and respond to people's tastes and preferences. Smart cities further interact with people and through this interaction; people can highlight areas that require improvements and adjustments.

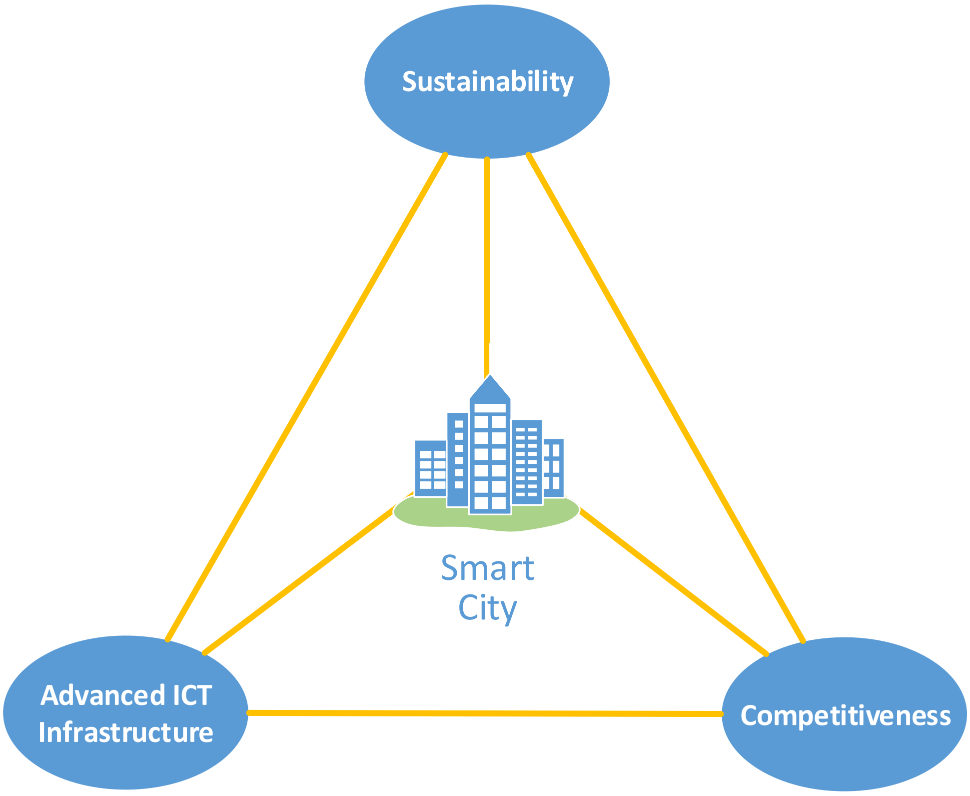

Figure 5: Objectives of a smart city.

2.2.3 Citizen-centric Smart Cities

A user-centric design is crucial when designing any product because it ensures that the final product meets the user's needs. Urban planning; just like any other planning is susceptible to bias and exclusion. Therefore, involvement of all stakeholders in making people-centric urban policy is very crucial in ensuring that the developed smart cities fulfil the appropriate human needs. As [9] stated, "***As the famous urbanists Jane Jacobs and Jan Gehl remind us****, "building cities should always begin with a consideration of the needs and behaviour of individual people, and then their interactions with their surrounding material environments, and each other*". When integrating the various digital technologies into our smart city echo-system, it is vital to consider the urban life to ensure that the included digital technology facilitates human coexistence and not hinder human beings from enjoying the smart city benefits. According to [33], building a smart city should facilitate the optimal use of technology and ideas to create an urban city conducive for all types of people. Building a citizen centric city involves factoring in different ecosystems and social spheres. Therefore, proper understanding of these complex interactions between different overlapping ecosystems is vital before introducing new technologies to them.

One strategy to ensure the people's interests are put first, is involving them during decision making process. Urban centres that have been developed with people's interest at the centre have resulted to very successful projects [9] [34]. Authors in [32] further suggests that the process of urban planning can be enhanced through the use of emerging technologies like social media that can help to engage with people. Use of such technologies can help the urban planners an opportunity to actively involve the local community in the planning process rather than just planning and then calling a consultative forum for the people to give their views after the plan have been already made.

In the end, directly or indirectly, the citizen is the primary beneficiary of all smart cities initiatives [35]. Thus, citizen participation in smart cities improvement and development is crucial to satisfy citizen needs. Speaking about IoT technology, it can be perceived as an enabler of active and passive citizen participation in smart cities development via participatory sensing and crowd-sourced data where city employees and citizens contribute to the data infrastructure of a city [36]. This approach allows smart cities to realize a variety of new applications created by local community groups without the need for ongoing coordination by governments.

2.2.3.1 Smart Seoul

Seoul in South Korea is among the smartest human-centric city with a population of over ten million [9]. It is advanced economic and tourist destination. Seoul is among the most tech-savvy cities worldwide and has made a big leap in incorporating smart technology. Seoul was not built as a smart city but its systems have been gradually made smart, a process called 'Smartization.' It also considered the most wired (connected) city as it has a fibre optic cable running through the city connecting all public amenities and having public Wi-Fi at public parks and places. Initially, Smart Seoul, then known as u-Seoul, was not human-centric as it just applied ICT on the existing traditional infrastructure, which improved service delivery in domains such as transport and safety but did not produce any improvements on the quality of life of the citizens. U-Seoul was basically a digitization of the existing infrastructure and resources.

In 2015, a human-centric Smart Seoul was introduced to ensure there was improved collaboration between the city and its citizens. Smart Seoul aimed at enhancing the city competitiveness, sustainability and the happiness of all its citizens [9]. Smart Seoul was built on three pillars: the ICT infrastructure, the integrated city management framework and the Users (Citizens). The last pillar was meant for the inclusion of the end users of the smart technology. The government had to prioritize and ensure that there is access and training on smart devices across all income levels and ages through a program they called 'smart devices for all.' Additionally, they ensured connectivity through free public Wi-Fi. Then the authority facilitated public data to reach all citizens. All documents with public information were made available online to ensure that all citizens have access. The citizens were then the actively involved in online engagements to share their views, opinion and ideas. The Smart Seoul project also focussed on safety featuring the children, the aged and the physically impaired persons. These people are voluntarily provided with a smart device and when they leave the designated safe zone the device sends an emergency alert [9]. Also, emergency buttons are placed on those devices or along streets and when pushed, they send emergency signal to the police, fire department and the control centres.

The Smart Seoul covers the safety perspective as far as persons with disability such as visual impairment are concerned. The trust model in this perspective is based on the systems trusting the data from the sensors in devices issued to visually impaired persons and the emergency alerts from those devices and other devices installed in public areas such as parks.

The trust between the users (child, impaired persons, caregivers, parents and the emergency control centres) and devices is built from reputation [9], whilst trust between the user devices and the control centres is built on contractual agreements between the manufacturer, users and the smart systems.

2.2.3.2 Ottawa Smart City

Ottawa [34] is the capital city of Canada with a population of over nine hundred thousand. It is both a commercial hub and a major tourist destination especially in summer. Ottawa is undergoing 'smartization' to as to improve the service delivery to its residents, to create a smart business environment and to improve the quality of life of its citizens. The project Smart City 2.0 was started in 2016 by both the public and the private sector. Smart City 2.0 focused on three goals;

- the connected City – to ensure that all citizens and businesses have efficient and affordable access to broadband network,
- the smart economy – to increase economic growth through supporting business expansion through smart technologies for local and foreign entrepreneurs and also support talent development, and
- the innovative government - to develop new and innovative ways of improving the lives of the citizens and their businesses through smart service delivery models, smart technological solutions and partnerships.

The technologies to be implemented in the smart city 2.0 includes IoT devices and networks. Sensors will be used in data collection. This means that the citizens and the government will have to invest in IoT devices such as CCTV cameras and LED light sensors among others [34]. More investment will go to storing and securing the data, big data, collected by the sensors. Trust model(s) will have to be developed to ensure that the system resources can trust each other and the citizens can trust the system.

Smart City 2.0 have planned to involve the citizens at different levels. First it aims to ensure that all the citizens have access to public data through usable application program interfaces (APIs) and interact with the data in real time. Secondly, it intends to continuously involve the residents in decision making in regard to the smart city systems through workshops and public forums where they air the problems they would like the smart city systems to address. Other means of engaging the residents are through hackathons, smart City website and through assessment using key performance indicators (KPIs) where the residents and partners evaluate the performance of the Smarty city [34]. Additionally, the education systems will embark in providing education programs, within the learning institutions, that will create a knowledge base that will promote the implementation of the smart city. Such programs include computer science, data science, business intelligent systems and machine learning. This will ensure many residents will able to contribute to the development and enhancement of the smart city. It will also improve citizen participation.

The Smart City 2.0 however, does not outline the incorporation of impaired person, children or the aged. It does not mention the inclusion of such groups but generally refer the users as the citizens [34]. These groups contain persons with special needs and require special attention, devise and infrastructure. Involving them in the design and development of the smart systems will help in developing smart systems that suits the needs of all citizens.

Furthermore, these groups will develop trust in both the devices and smart city systems and be able to interact freely.

3 Literature Review

3.1 Existing trust models

3.1.1 A Trust Model for Data Sharing in Smart Cities

In [36] it is observed that there is an increase in data generated by the existing IoT infrastructure and devices. These data should be shared among the various applications in the application layer. However, trust issues arise when sharing this data and this prevents IoT from achieving its full potential. As a result of the mistrust, there is need to have a trust enabled strategy to facilitate data exchange. These strategies include data perception trust, trustworthy data mining and concrete trust related policies [36]. Due to the issues highlighted above, [36] proposes data sharing trust model that focuses on transparency and accountability. The proposed model captures the various data constraints, restrictions and obligations imposed on the data users. However, the model does not include a data usage transparency but instead introduces a shared platform architecture to help stakeholders participate in the various strategies set aside to facilitate data usage transparency and accountability.

The authors introduce the trust ontology concept that is used to represent data usage control requirements concept, to annotate data generated by IoT devices in the smart cities. The semantic model is used to represent the number of entities and the states of these entities. This new model enhances flexibility in data integration and data processing. Trust enforcement is also provided for the shared data depending on the consumer's preferences and the data owner's policies. Trust enforcement enables the IoT shared platform to monitor the history of data usage.

3.1.2 Trust model system architecture

3.1.2.1 Layers

Infrastructure layer – this is the bottom layer and it comprises of the various IoT devices that are set up to send data to the various applications. The IoT objects in this layer can be from various domains which include smart sensors, smart street sensors or smart alarm systems.

Platform layer – This is the middle layer and comprises of four functional entities. These entities include *Ontology Manager (OM), Application Manager (AM), policy manager (PM) and data manager (DM)* [37]. The PM works closely with the trust policies while the DM handles the IoT data. The AM operates the available applications in the IoT infrastructure.

Application layer – this layer contains the end-user applications. These applications receive the data sent by the DM through the platform.

3.1.2.2 Semantic and Abstraction

Data integration – semantic technology is used to enhance data consistency among the various heterogeneous data set schema. The model further proposes the use of Resource Description Framework (RDF) that helps to in encoding the transmitted data and resources. The RDF further facilitates quick integration of various vocabularies.

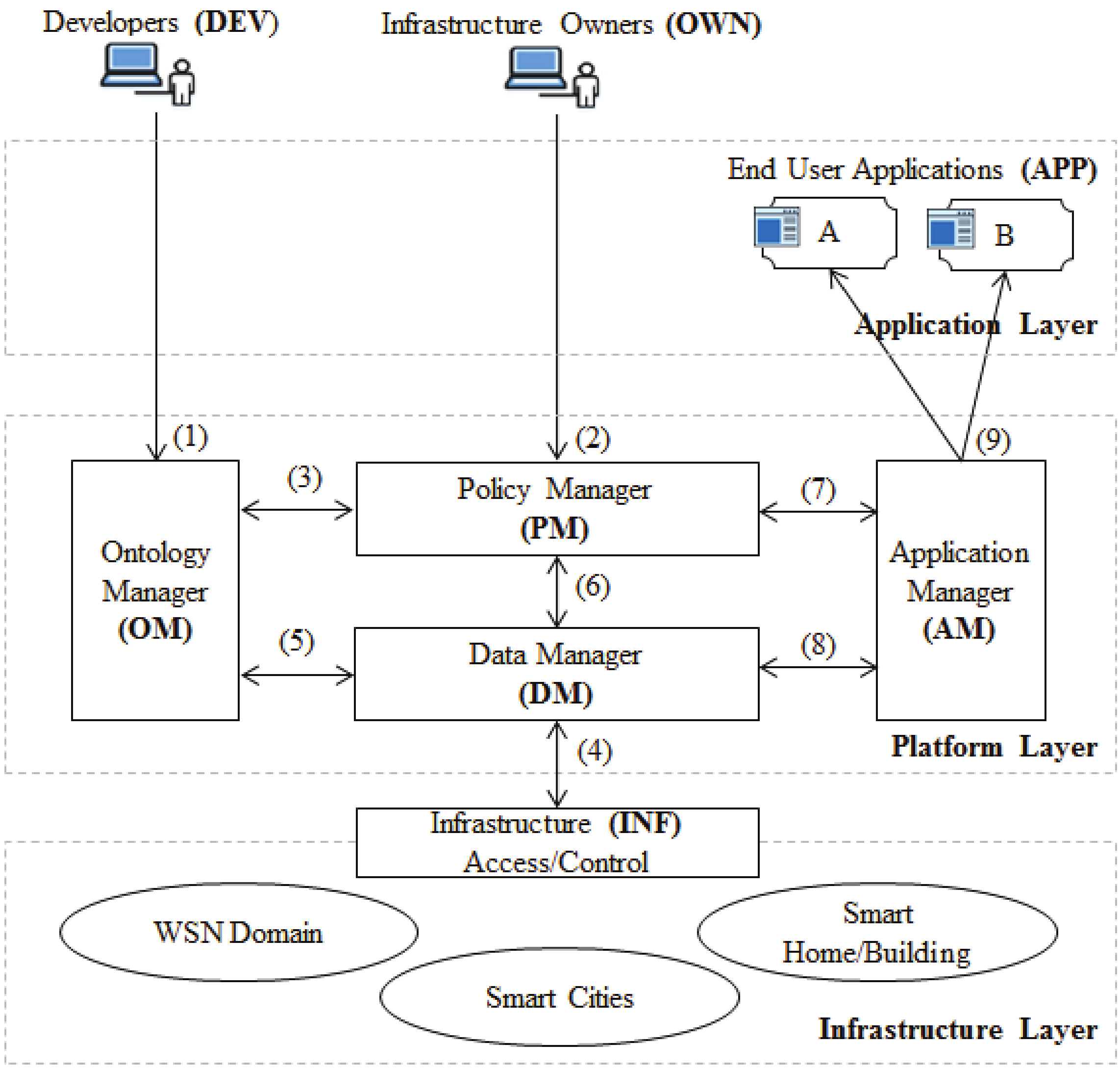

Figure 6: Trust Model system architecture.

Data modelling – the authors propose a semantic language to assist in modelling the entities available and the entities' state for the sent data or resources. The semantic language facilitates interaction with high-level entities instead of interacting directly with the IoT devices. [38] indicates that they are working to develop ontologies for different domains and they are waiting for standardization form the W3C. Some of the developed ontologies include Smart Appliance Reference (SAREF) ontology that was developed by TNO and it caters all sensors and actuators.

Data processing – various semantic web technologies are used to retrieve IoT data. These technologies include SPARQL which is database language like SQL and facilitates querying of an RDF store. This language also facilitates logical reasoning which makes it possible to infer knowledge from existing rules.

1.1.1.1 *Transparency and Accountability*

Mechanism – the figure above illustrates the sequence of enhancing transparency and accountability. The OM manages trust ontology to provide TDU. The PM then manages trust policies from the data provider where the infrastructure owner (OWN) is presumed to be the data owner.

Trust Ontology – the author proposes a trust ontology referred to as TDUO. In this ontology, the usage policy is defined by modal operators that include *Obligation, Forbidden* and *Permission* on various conditions such as *class of actors, constraints, and class of purpose.*

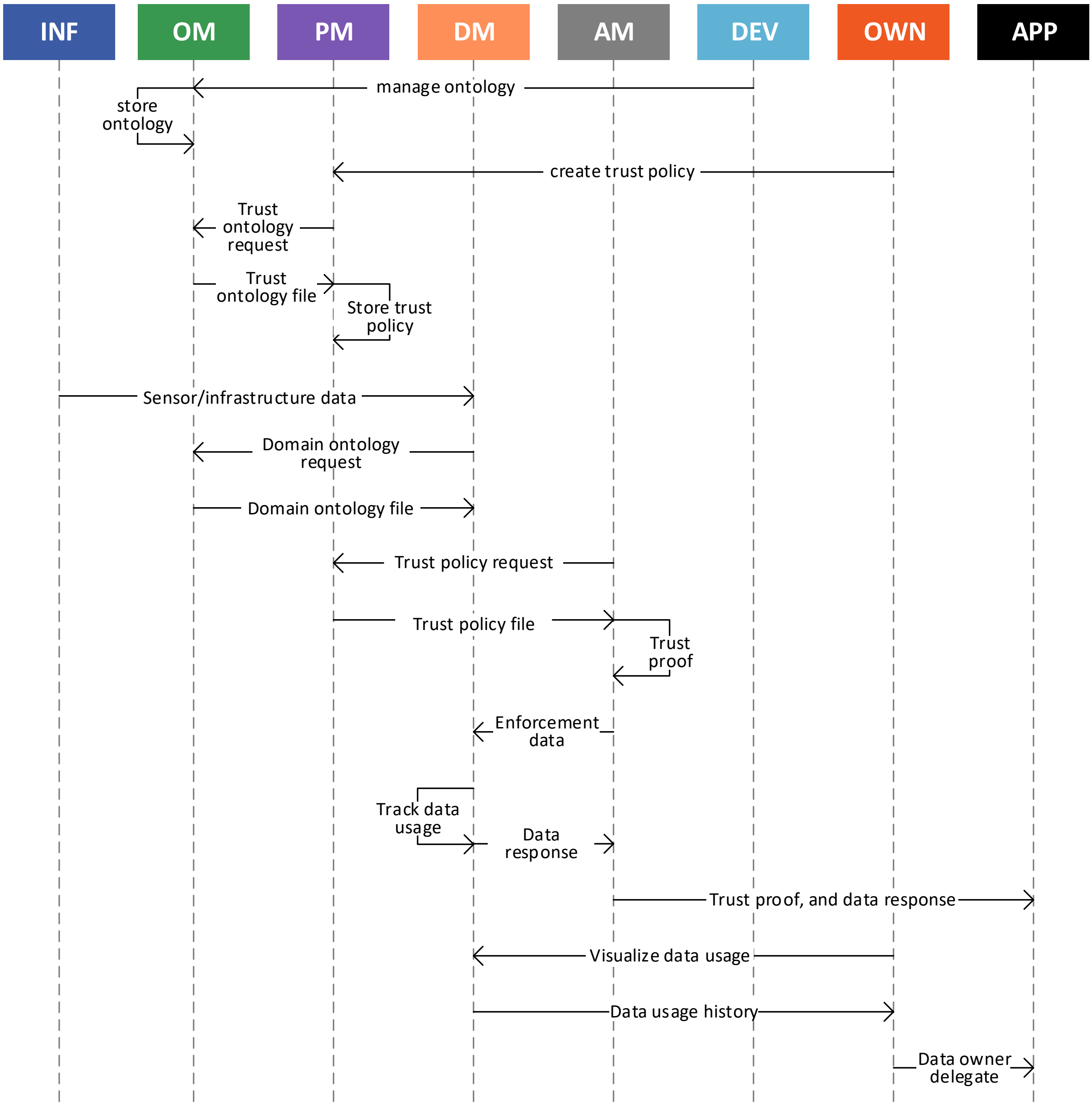

Figure 7: Transparency and Accountability.

1.1.1.1 *Experiment results*

An experiment was carried to test the proposed model. The confidence interval for all the results was above 95%. The trust enforcement request delay was noted to be 20ms. This meant that the proposed trust enforcement model did not introduce much delay.

3.2 Trust-based Discovery for Web of Things Markets

In [39], the authors discuss the current components of trust-based discovery in web of things. Then, they propose other measures that should be adopted to enhance the trust-based discovery of products and services on the Web of Things. The Web of Things is composed of various markets where traders exhibit their products and sellers engage in purchasing products. E-commerce has evolved since the introduction of online payment processing systems where payments can be made through mobile phones or credit cards [39]. As a result, online shopping has increased a lot in recent years. The authors further observe that the Web of Things involves interaction of data and Service APIs that process those data and facilitate user interaction with the online systems. Users, at times, can submit sensitive data including credit card details, personal identifiers or regular search phrases and commands. A certain level of trust is required in order to facilitate these interactions.

Currently, there existed IoT market places that it is believed that these might grow and become Web of Things market places. These online market places will facilitate the trading and publishing of data and services for Web of Things. However, the management of trust will be a major issue in the web of things. Authors in [39] indicate that the challenges like trust management and trust negotiation for the Web of Things market place, are based on the fact that there is no central authority to control the traded products. In the Web of Things, users will be required to search for products based on particular needs and expectations like convenience, price, delivery location, payment terms and so on. However, in case of sensitive data or critical search criteria, trust polices and expectations must be put into consideration and, thus, only products that have trust guarantees are considered.

The authors observe that a reputation-based trust mechanism is essential to facilitate web of things market place. Trust management and trust negotiation in the Web of Things are different from the traditional market places that include e-commerce market places such as Amazon. The difference comes in because the traditional market places use trust based mechanisms that are based on reputation, reviews and user ratings. Users use these reviews and ratings to evaluate the trustworthiness of a seller or a product. However, in the case of Web of Things, the trust mechanism is bidirectional. This means that both the objects and services must have trust towards each other. Sellers and buyers must trust each other.

Trust model in the web of Things includes other indicators such as "*security and privacy guarantees, quality of a service or device, or quality of the data* [39]*.*" To effect these indicators, various security protocols such as SSL, key exchange mechanisms like AES and specific certificate providers such as Go Daddy. The security protocols will act as trust mediators where each entity is verified based on a set standards [40]. The trust indicators may vary depending on the user, the user's past experience or context. These variations make it crucial to develop appropriate trust management and trust negotiation strategies to facilitate proper and accurate evaluation of trustworthiness of the products in the web of things.

3.2.1 Components of the trust-based discovery

In [39], the use of semantics is proposed for the introduction of formal vocabularies to describe the expectations of various contexts. The service providers should have a semantic means of describing trust guarantees of their objects and services. Existence of these formal semantics will facilitate matching of the trust expectations and trust guarantees. The authors propose a trust ontology to be developed and integrate it with other existing ontologies relevant to this trust model. The trust ontology will help capture the semantic of trust, and trust models, like the Trust Relationship, Trust Participant, Trustee expectations, Trust guarantees, Trust Attribute, Measurable Trust Attribute, Non- measurable and Trust Attribute [39].

The process of discovering trustworthy products for the web of Things is referred to as Semantic matching. The trust expectations of the users are matched with the trust guarantees of the web of things products. A product is marked as trustworthy if the trust expectations matches the Web of Things trust guarantees. If the trust expectations do not match the trust guarantees, the product is labelled untrustworthy. Proper standardisation of trust guarantees and trust expectations, using semantic vocabularies and other machine annotations, will make it possible to develop the trust based discovery model. Coupled with the existing semantic matchers, the trust-based discovery model can be enhanced to facilitate the matching of trust expectations with trust guarantees.

In order to increase efficiency, a central organisation or users should constantly monitor the trust guarantees. The monitors will help verify the trust guarantees. The trust guarantees should be monitored with the use of sophisticated strategies and use of third parties to help detect, separate and restrict the unrequired behaviours.

3.3 TrustyFeer: A Subjective Logic Trust Model for Smart City Peer-to-Peer Federated Clouds

The authors [41] propose a trust management system for peers in a federated cloud that is adopted in order to achieve the goals of smart cities. A federated cloud has several independent cloud service providers (CSPs) who are in agreement to share their infrastructure and services so as to provide a wide range of resources to their customers with a high quality of service (QoS). With each CSP bringing its resources on board, every other participant is able to access a larger pool of resources to enable them handle peak load without necessarily having to add more resources. With this sharing of resources, trust is very important from one peer to another. The sharing and the independent provisioning of resources require trust among the CSPs to prevent malicious activities by any CSP.

In the proposed trust management system, the peers' trustworthiness is ascertained using subjective logic opinions that are obtained from the peer's reputation and the service level agreements (SLA). The proposed TrustyFeer trust management system comprise of the system registry, a reputation database and a provider peer. The system registry is an in-memory database that stores the list of the participating CSPs, otherwise referred to as peers, and the resources they offer [41]. The reputation database contains the so called reputation matrix which is regularly updated. The provider peer contained the trust manager, service manager, calculations manager and the opinions database. The service manager receives requests for services, rates, normalizes and lists them, then sends the scores to the trust manager. The trust manager receives the scores and is responsible for trust calculations. It uses a transitive trust calculator – summarized below - to calculate indirect trust and a parallel trust calculator to calculate parallel trust.

This system calculates, belief, disbelief, opinions and uncertainty using subjective logic that is based on new trust formulas and weight trust values. These values are based on the global reputation of each peer and how the CSP conforms to the SLAs. This enables TrustyFeer to build a trust overlay network (TON) which enable participants build their trust and be evaluated by their peers based on their interactions with each other. The authors then evaluated the performance of this trust model by comparing its performance with two trust systems, EigenTrust and TNA-SL, TrustyFeer emerged to be the best in all tests producing the most reliable trust results given varying number of peers and threat models [41]. TrustyFeer also produced the least results of untrusted CSPs. This trust model gives a new method of calculating trust while considering the CSPs reputation and the SLAs. It has increased the level of trust calculations to ensure untrusted CSPs are not entertained in the federated cloud.

3.3.1 The ConTrust Model

Privacy is a crucial component in enhancing security. Security focuses on preserving crucial information so that users can freely share sensitive information without fear of access by unintended parties. The authors in [9] define privacy as "*The right of an entity (normally a person), acting on its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others.*" To enhance privacy, various strategies like data encryption, restricting access rights and implementing authentication mechanisms can be utilized. Using ConTrust [42] as a security component is vital in success of IoT as it facilitates to limit malicious objects from entering the IoT environment. Use of ConTrust further helps to prevent various attacks such as trust-based attacks that might interfere with the right trust reputations of a particular object.

IoT objects have different features compared to other internet objects and as such, trust is needed for these objects to interact harmoniously. New IoT objects are developed each day and as a result, objects can enter or leave any IoT environment at any time. Therefore, due to the dynamic nature of IoT objects, proper trust mechanisms must be put in place to ensure the generated trust recommendations are accurate [9].

The ConTrust model has four processes;

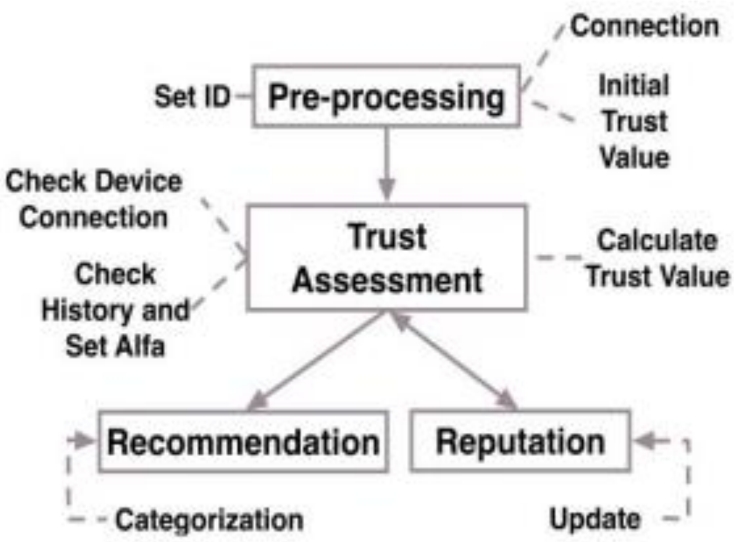

Figure 8: ConTrust model processes.

3.3.1.1 Pre-processing and Trust Assessment

These processes includes objects modelled using the paradigm of the Social Internet of Things (SIOT) [43] where the available users can possess more than one object and the available objects can enter or leave a community based on its preference. Each object has an ID for identification purposes. The ID contains the object number and other user information. An object's initial state comprises of three matrices; other objects' reputation value, the object's trust value and information used for connectivity purposes. This process has a function that helps in computing the object's trust value. The functions can calculate values for objects in the same or different community.

3.3.1.2 Recommendation

This process uses the trust value estimated in the pre-processing and trust assessment process to recommend the object for consideration. The recommendation value can either be very trusted, trusted, untrusted or very untrusted. Based on the recommendation, an object profile value is assigned. The profile value helps in determining the reputation process of a particular object.

3.3.1.3 Reputation

An object's reputation can be estimated through past experiences and current object interactions. The reputation then is used as a parameter when estimating an object's trust level. A Dynamic Trust Mechanism can facilitate in estimating the trust level that can be used to select the IoT devices [9]. The trust value can also be estimated using past experiences or through appraisal from other people.

3.3.1.4 Results and discussion

A ConTrust simulation was conducted to verify the model. Changing the object parameter values affected the trust value. Use of a trust assessment method in the ConTrust model may lead to more stable results. The reputation parameter helps to stabilize the reputation values. The inclusion of time parameter in the ConTrust model stabilized the reputation values.

3.3.2 Trust-based Discovery for Web of Things Markets

Internet of Things is composed of multiple objects that need to be secured. Securing these objects involves developing structures for data encryption, enhancing privacy and trust management mechanism. Authors in [42] proposes the development of a ConTrust model that helps to ensure that only trusted things are accepted in the IoT environment. The ConTrust model utilizes current trust assessment and the reputation history. In [44], the old market places like Amazon relies on user ratings and reviews to enhance trust. Use of user ratings and reviews as a trust catalyst brings out the concept of time that the ConTrust model seeks to incorporate to facilitate accuracy in trust estimations.

There is a wide range of opportunities in the Internet of things (IoT), but its market scope is constrained by heterogeneity. Its constraints are evident as products and/or services from different manufacturers are merged into a single application or process. Nonetheless, there are tremendous prospects for systems that incorporate sensors, actuators, and several information sources. The Web of Things (WoT) aims at combating the complexity of the IoT by simplifying the integration among systems and applications. A straightforward definition of the WoT is given below.

"The Web of Things (WoT) is a computing concept that describes a future where everyday objects are fully integrated with the Web. The prerequisite for WoT is for the "things" to have embedded computer systems that enable communication with the Web. Such smart devices would then be able to communicate with each other using existing Web standards [45]".

The WoT is concerned with the highest layer (i.e. Application layer) of the OSI model [46], handling only applications, services, and data. Consequently, developers do not have to deal with problems coming from the physical characteristics of various IoT devices and the transport/network protocols they use (i.e. layers 1-6 of the OSI model). A virtual representation that maps IoT devices into software objects almost obliterate networking constraints and improve growth capacity. In other words, the consolidation of the IoT and the

Web expands the spectrum of traditional web services from strictly cyber to cyber-physical services.

Such systems are typically built by combining different services with additional functionalities to ensure that the resultant structure is secured and versatile. An example of that service-oriented ecosystems is the COMPOSE [47] project. The main objective is to allow users to create new applications using current services deriving from Web APIs, sensors and mobile devices, or other resources. In a decentralised system, like the WoT, managing thrust among the entities can be very challenging.

Comparing traditional E-commerce Marketplaces, like Amazon, and WoT Marketplace we notice that the trust relationships are unidirectional and bidirectional respectively. The former, use reputation-related mechanisms like reviews and ratings so that users can evaluate the trustworthiness of a product and/or a seller. On the contrary, since WoT Marketplace entities can be end-users, developers, sensors, services, etc., trust is considered mandatory from both sides (i.e. provider-consumer). For example, a sensor should guarantee good Quality-of-Data (QoD) to be trusted from an end-user while at the same time provide with its data only trusted, authorised end-users.

According to the above, the success of WoT Marketplaces relies heavily on the trust between the platform and its users. The variety of users (e.g. objects, individuals, public or private organisations, developers, services, etcetera) results in different security and privacy requirements such as, secure data processing, prevention from information disclosure, and protection from potential malicious actions, to name a few. The fulfillment of security and privacy requirements in conjunction with good reputation, Quality-of-Service (QoS), and Quality-of-Data (QoD) are the indicators of trust expectations. To conclude, trust is a subjective notion, highly dependent on the type of the user, and the context of the product/service in exchange. For that reason, trust should be treated properly during the discovery and composition in order to enable its appraisal of the WoT users and services.

The methodology for building efficient trust-based discovery engines for the WoT is simple but not simplistic. This methodology is based on semantic matching processes and its key elements are the following three:

- Semantic vocabularies and sematic annotation
- Semantic matchers
- Monitoring

In practice, first thing to do is design semantic vocabularies of (context)-specific trust expectations clearly stated by both users and providers. The former should clarify the trust expectations, and the latter the trust guarantees. If those clarifications can be expressed in a formal and common way, then the trust-based discovery mechanisms will compare them and conclude if and in what level (fully, partially, not at all) they match.

A variety of factors must be considered to build a multilateral trust ontology. The authors in [48] suggested a model that separates the trustor from the trustee, while also identifies the type, the scope, and the value of the trust in each case, as well as the intermediate trust processes (i.e. policy-based, reputation-based, and evidence-based). A similar approach is presented in [49] where the defined thrust ontologies are destined for service-oriented environments. These techniques cover a respectful range of trust-related factors, however, there are a lot more to take into account. W3C Semantic Sensor Networks (SSN) Ontology [50], for example, provides concepts that may be relevant to a sense of trust in sensory devices such as accuracy, detection limit, drifting, frequency, latency, resolution, and sensitivity. Existing QoS ontologies, such as WS-QoSOnto [51], can be reused to characterise quality services based on trust standards, which were originally designed to address quality aspects of semantic web services.

As we have seen so far, services released in WoT Marketplaces should be defined in a manner that enables their discovery not only in compliance with operational constraints but with security requirements too. Unified Service Description Language-Security (USDL-Sec) [52] specification is suggested as a method where service providers define security features (privacy and authorisation) of their services, whereas the consumer relies on Security Certificates (Asserts) that provide him with the assurance and the level of 'matching' between the provided services and his/her requirements (in terms of security). Another example of semantic matching mechanisms is the Web Service Trust Ontology (WSTO) [53] that manages trust in web services. In case a match is detected, then a scale from 0 to 1 reflects the level of trust.

Continuous and regular verification and monitoring of the trust guarantees, by users and/or third parties, is considered to be equally critical. The related mechanisms will gather evidences from various sources which may include reputation-related techniques, popularity and QoS/QoD evaluation, etc.

To summarise, the WoT marketplace is a complex system, highly depending on the context of applications and the bidirectional relationship between its users. With trust being the key element for this concept's success, the first goal to be met is the formation of a structured formal vocabulary so that providers and consumers can state and acknowledge the trust requirements and guarantees of the products/services in transit.

3.3.3 Components of the trust-based discovery

Service providers should use the same language as end users to state the trust guarantees that describes formal semantics [54]. It should be defined what is ensured and how.

Discovery of trustworthy products is known a ***semantic matching*** task [54]. The components allow to map user expectations into trust guarantees of a Web of Thing product are ***semantic matchers***. The component responsible for matching realizes a classification task where each product needed to be classified as trusted or not - the level of trust is always a value between 0 and 1. The trust classification engines that realize this task can be significantly improved be using semantic vocabulary and machine-processed semantic annotations.

The measure of trust should be well defined by formal means to ensure a high security level. Exemplary different trust requirements are shown in Figure 9.

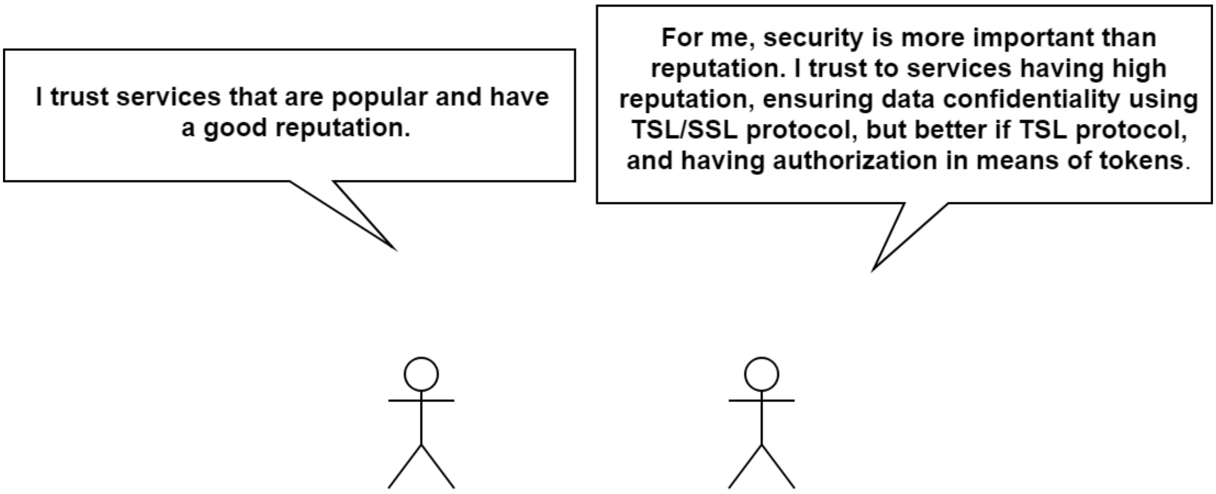

Figure 9 Visualisation of informal trust requirements (based on [54])

The trust guarantees should be constantly verified by users or by established central authorities. The **monitoring** task is collecting the evidence for the claimed trust guarantees. The monitoring of trust guarantees requires sophisticated mechanisms over the Internet with possible involvement of trusted third parties for detecting and reacting to them - isolating and limiting the negative behaviours. The evidence of trust guarantees may be coming from different sources including:

- users reviews and ratings,
- various estimations such could be an estimation of popularity,
- third party services assessing the quality of services and data (e.g. detection of accuracy of a humidity sensor by comparing the data with the data of other humidity sensors in the same area),
- third party services performing static code analysis to detect possible negative effects of the execution, etc.

4 A trust model example: Assisting the mobility of the visually impaired

4.1 The visually impaired

There is an estimated 1.3 billion people in this world with visual impairment conditions. Out of these, 36 million people are blind while 26 million people have near vision impairment [55]. According to the Iowa department for the blind, a visually impaired person is considered to be legally blind if their vision measures 20/200 or worse [4]. Blindness can be caused diseases or physical injuries. As technology evolves, various technologies have been invented to help the blind in the society. However, despite the current measures to assist the blind people, they continue to face various challenges. In this section, we will discuss the challenges faced by the blind people and then discuss how IoT can help the visually impaired.

4.1.1.1 Environment

According to the World Access for the blind, majority of the blind people find it difficult to walk around. Blind people face difficulties when self-navigating in familiar and non-familiar places or when walking in crowded places. This is why the visually impaired mostly brings friends along to assist them navigate in unfamiliar places. Blind people also have to learn how a particular place is organized. If for example a table is moved in the house from the usual place to another, blind people find it difficult to locate it. These means that current environments only favour blind people when they are static. In a research conducted [55] regarding *"Mobility-Related Accidents Experienced by People with Visual Impairment."* The research revealed that blind people suffer from the risk of falling and collisions while walking. The survey involved 300 legally blind people and some of the findings are discusses below.

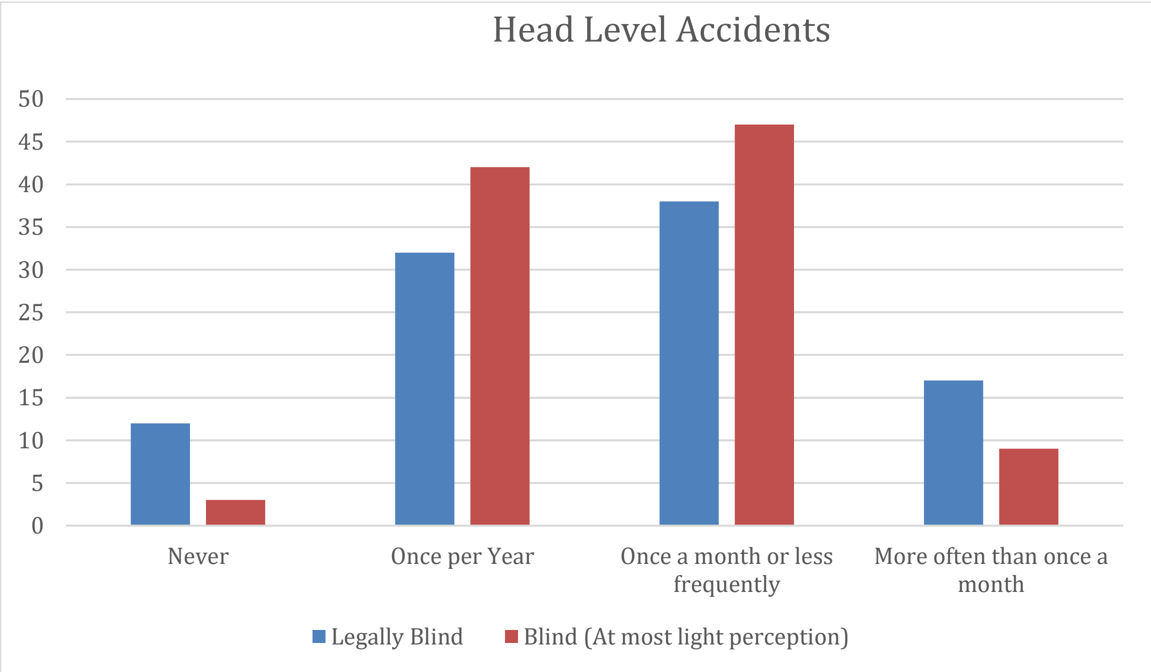

Figure 10: Head level accidents frequency distribution [55]

According to the survey results, only 2% of the entire blind population never experienced head level accidents compared 12% of the legally blind people. This means that 98% of blind people and 88% of legally blind people have experienced head level accidents in their entire life. The survey further revealed that only 17% of the legally blind people do not experience head level accidents more often than once a month while in the case of the blind people only 9% that do not experience head level accidents more often than once in a month. In other words, 83% of the legally blind people experience head level collisions more than once a month [45].

Out of these accidents, 23% required medical attention. Some of these victims required stitching while others required home rests. Apart from accidents, some of the other consequences of these accidents include loss of time, missed appointments or taking time off. The high level of accidents affecting the visually impaired people in the society requires a comprehensive approach. If at all the smart cities are going to be smart, then they must be responsive to the needs of the blind people. Blind people’s lifestyles must be captured during the initial stages of the city’s design.

4.1.1.2 Social

According to the World Health Organization, blindness limits a person’s capabilities and thus denies them numerous opportunities. Visual impairment hinders a person from involving in activities outside their place of work like sports or enjoying themselves in a social gathering. The fact that the blind person is unable to engage in these duties eventually lowers their self-esteem. According to [4], a man named Eric Burton, was not blind but was born with a health condition; Retinitis Pigmentosa that worsened at the age of 35 and eventually turned him into a blind person. He tried various technologies but none succeeded. When his wife requested him to try a new product between her company AT&T and AIra Agent; a remote guide who assists blind people to navigate various environments by describing their surroundings using a cellular. Burton was hesitant at first and said *"Blind people get tired of everyone trying to ‘fix' them, I've tried so many things, only to end up frustrated with my hopes dashed."[55]* However, Burton later yielded after facing difficulties navigating through a crowded place. Burton’s sentiments indicates a dejected person who is almost losing hope and this reflects other blind people’s feelings across the world.

4.2 Smart cities for the Visually Impaired

The challenges experienced by the blind people highlights the need for Citizen-centric smart cities. Developing the smart cities and factoring in all kinds of people in the city will facilitate to reduce the massive gap between those who can see and the visually impaired. One of the main challenges for the blind people according to the World Access for the blind is movement [6]. In a smart city, movement is not only walking, but it also involves driver-less cars and riding to say the least. In addition, current technologies do not provide contextual information to the visually impaired, depriving them from developing situational awareness. This is particularly critical as current technologies do not accommodate how the visually impaired should react or be handled in case of, say, an emergency. Example of emergencies include riots, attacks, when their visual aids fail or a building collapsing. These challenges create the need for citizen-centric cities where the visually impaired can use technology to depend on themselves instead of relying on family members, friends or well-wishers.

4.2.1 An architecture for the visually impaired

The visually impaired people are belong to a special group of people that require an effective IoT system to ensure that their wellbeing and success is catered for. Ambient intelligent systems are crucial in facilitating safe and comfortable coexistence of the blind people. The Ambient intelligent Systems (AMIs) are sensitive and responsive to a persons need based on how they interact with the environment [56]. The AMI utilizes context-aware technologies that perceive stimuli from users as they interact with the systems [7]. The main purpose of living assistance systems is to help the disabled achieve individual benefits, become economically empowered and uplift the society through improved living standards. The AMI systems are integrated with smart objects to form the IoT.

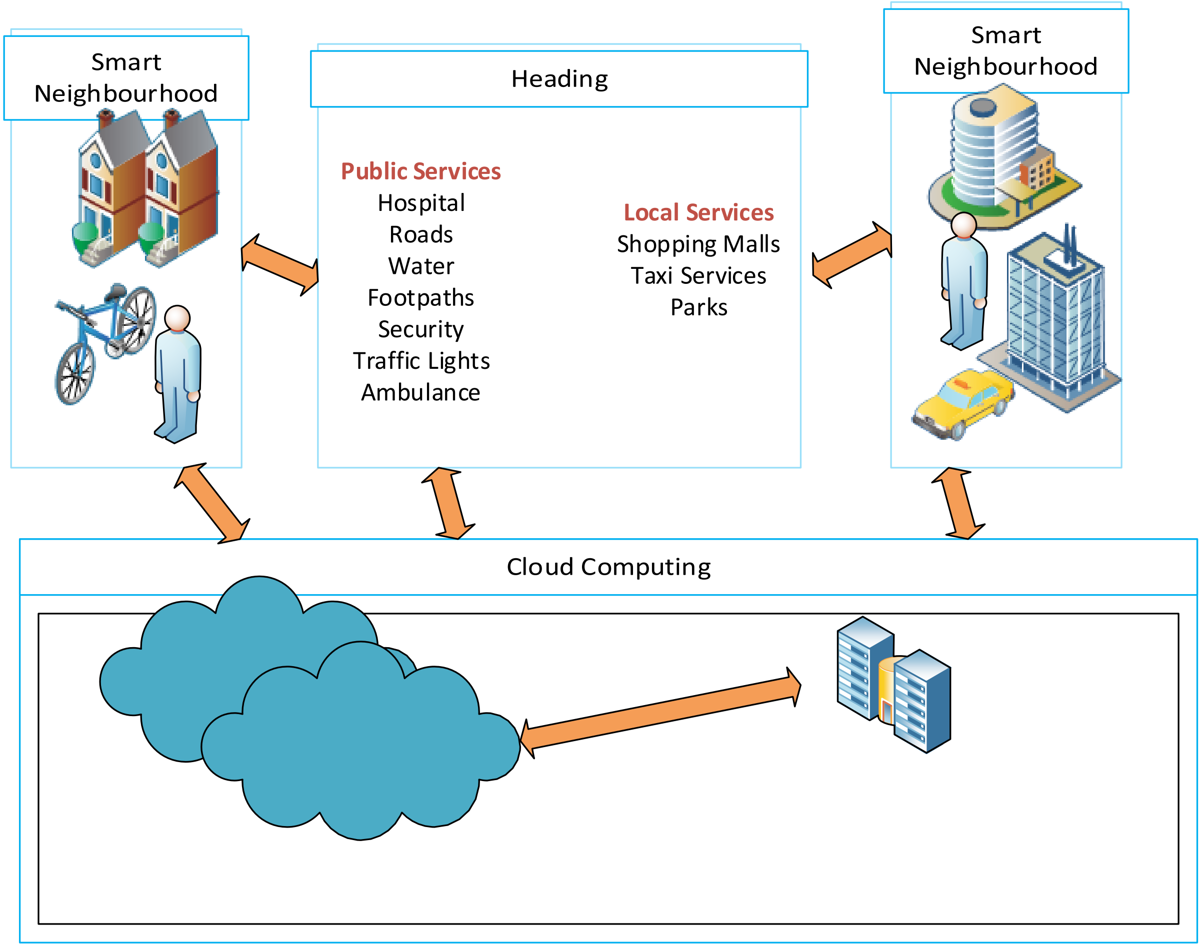

Figure 11: Citizen-Centric city Architecture

4.2.2 Essentials for the Visually-Impaired Trust Model

4.2.2.1 Semantic Vocabularies

As observed above, for a citizen-centric city to work effectively, there must be trust between the trustee and trustor [56]. As a result, there should exist standards that can be used across the board to express particular trust expectations. For example, *'safe roads have a foot path and a path for riding bicycles'* or *'good libraries have a brails section'.* With the same respect, the local authorities should indicate the trust guarantees to the blind people. For example, as indicated by [32], movement is one of the major challenges experienced by the visually impaired. Therefore, the local authorities should have mechanisms of updating the blind people of the appropriate time to walk. For example '*Do not use 5th Avenue Road Tomorrow, there will be demonstrations*'.

One Ontology developed by W3C is the sensitivity Ontology [38]. This ontology, among others can significantly help in developing the visually impaired trust model. This is due to the sensitive nature of blind people. By factoring in the special nature of human beings, it will help give appropriate feedback and instructions regarding different scenarios [57]. Due to the invention of various technologies for the blind people like the Bluetooth enabled Lechal shoe for the blind [58], it is difficult to recognize a blind person since they do not have to use a walking stick. Therefore, a blind person should have a device like a wrist band with a sensor that communicates with other sensors. The sensitivity ontology can be enhanced to enable objects in an IoT environment to trigger emergency alerts. For example, if a traffic sensor detects a blind person's sensor crossing the road, an extra security light should appear to inform the drivers that there is a blind person crossing the road. This can be helpful if the blind person is not using a walking stick. The experience ontology should be introduced to capture past experiences and perceptions. The past experiences dictate how the blind people will react on certain circumstances.

As indicated in [9] regarding the Smart Seoul city, the government might opt to license private companies to provide some services on its behalf. These services might include alarm systems or emergency buttons monitoring services that are used when a blind person leaves a designated safe zone. Also, the government works in collaboration with other private sector players like clinics for emergency response cases. As a result, a data sharing model must be established between these entities. Apart from the data sharing model, a special agreement must be established between the local authorities and the subcontracted companies. The subcontracted entities ontology must be factored in the trust model. This is because subcontracted entities carry more responsibilities compared to other service providers. The blind persons will have to deal with the subcontracted entities since they provide services and things on behalf of the government.

4.2.2.2 Semantic Matchers

This involves the process of looking for trustworthy things in the citizen-centric smart city environment. The trust expectations of a blind person are aligned with the trust guarantees of a smart city [9]. As indicated, each blind person has their expectations and other standard expectations like any other normal human being. The smart cities also have their own trust guarantees in form of the things and services they provide. The smart city's things and services are identified as trustworthy if the trust expectations match, otherwisethey are labelled untrustworthy. The trust score (either 1 for trustworthy or 0 for untrustworthy) make it possible to provide guidance to the blind people as the sensors communicate and share data.

4.2.2.3 Monitors

The citizen-centric smart city is a concept that is still in the initial stages. Therefore, constant monitoring of the city's trust should be conducted. The provided things and services should be evaluated to determine whether they meet their expected goals. Accredited third parties should be involved to ascertain the set trust guarantees. Other monitoring avenues include user reviews and ratings and technological innovations.

5 Conclusion

IoT infrastructure facilitates the interaction between the humans and sensors and devices. Privacy, security and trust are crucial pillars for the holistic development of the IoT, since the collection and aggregation of data from various physical environments varies and differs in terms of risks and impacts overcoming uncertainty. A trust platform design based on a trust model foundation, which considers the infrastructure as well as the humans as the ultimate target is the constant increase of the city's sustainable growth and strengthen city functions, while guaranteeing citizens happiness and wellness.

Proper documented processes and infrastructure construction according to the standards and European related frameworks increases the trust thus the enabling of a holistic strategy to facilitate data exchange under a secure, private and trust pillars.

Citizen who is actually the primary beneficiary of all smart cities initiatives requires a platform functioning under zero weaknesses as threats might increase the risk and the impact to their privacy, security, trust and safety or even face any improper or lacking design and functioning of the platform.

Therefore, user-centric design is crucial upon designing and constructing a smart city platform. Services and products should be designed and planned according to accurate risk assessment, analysis and evaluation primarily executed from the design stage satisfying the needs and expectations of the users.

Vital approach of prerequisites are the documented information derived, for example by standards, such as policies (e.g. concrete trust policies) and implementation and comply of law guidelines and regulations (e.g. trustworthy data mining) in relation with the integrated city management approach (e.g. data perception trust and training).

6 References

[1] R. Cowley, S. Joss and Y. Dayot, "The smart city and its publics: insights from across six UK cities", Urban Research & Practice, vol. 11, no. 1, pp. 53-77, 2017.

[2] Truong, N.B., Um, T.W., Zhou, B. and Lee, G.M., 2017, December. From personal experience to global reputation for trust evaluation in the social internet of things. In GLOBECOM 2017-2017 IEEE Global Communications Conference (pp. 1-7). IEEE.

[3] A. Ramadhan, "Wearable Smart System for Visually Impaired People", Sensors, vol. 18, no. 3, p. 843, 2018.

[4] A. Blankson, "A New Vision For The Future: An IoT Solution To Assist Blind People With Sighted Support", Forbes, 2018. [Online]. Available: https://www.forbes.com/sites/amyblankson/2018/05/31/a-vision-for-the-future-iot-solution-gives-sight-to-the-blind/#8ae878d26c7d. [Accessed: 21- Nov- 2018].

[5] L. Auberger, "How AI and IoT help blind people to explore the world", Internet-of-Things.blog, 2018. [Online]. Available: https://internet-of-things.blog/en/how-ai-and-iot-help-blind-people-to-explore-the-world/. [Accessed: 21- Nov- 2018].

[6] Vanishree, M.L., Sushmitha, S. and Roopa, B.K., 2017. Addressing the challenges of Visually Impaired using IoT. International Journal on Recent and Innovation Trends in Computing and Communication, 5(1), pp.182-186.

[7] M. Eremia, L. Toma and M. Sanduleac, "The Smart City Concept in the 21st Century", Procedia Engineering, vol. 181, pp. 12-19, 2017.

[8] F. Gómez Mármol and G. Martínez Pérez, "Trust and reputation models comparison", Internet Research, vol. 21, no. 2, pp. 138-153, 2011.

[9] Hwang, J.S. and Choe, Y.H., 2013. Smart Cities Seoul: a case study. ITU-T Technology Watch Report.

[10] Coetzee, L. and Olivrin, G., 2012. Inclusion through the Internet of Things. In Assistive Technologies. InTech.

[11] Schuler, D., & Namioka, A. (Eds.). (1993). Participatory design: Principles and practices. CRC Press.

[12] Ncube, C. (2011, August). On the Engineering of Systems of Systems: key challenges for the requirements engineering community. In 2011 Workshop on Requirements Engineering for Systems, Services and Systems-of-Systems (pp. 70-73). IEEE.

[13] Weidlich, D., Cser, L., Polzin, T., Cristiano, D., & Zickner, H. (2007). Virtual reality approaches for immersive design. CIRP annals, 56(1), 139-142.

[14] Ali, R., Solis, C., Salehie, M., Omoronyia, I., Nuseibeh, B., & Maalej, W. (2011, September). Social sensing: when users become monitors. In Proceedings of the 19th ACM SIGSOFT symposium and the 13th European conference on Foundations of software engineering (pp. 476-479). ACM.

[15] Mazeiar Salehie, Ladan Tahvildari. Self-adaptive software: landscape and research challenges. ACM Transactions on Autonomic and Autonomic Systems, 4:2, pp. 1-42, 2009

[16] Kephart, J. O., & Chess, D. M. (2003). The vision of autonomic computing. Computer, (1), 41-50.x

[17] Ali, R., Solis, C., Omoronyia, I. , Salehie, M. and Nuseibeh, B. (2012) Social adaptation: When software gives users a voice. In: 7th International Conference on Evaluation of Novel Approaches to Software Engineering, Wrocław, Poland, 29-30 Jun 2012.

[18] Surowiecki, J. (2005). The wisdom of crowds. Anchor

[19] Fogg, B. J. (2002). Persuasive technology: using computers to change what we think and do. Ubiquity, 2002(December), 5.

[20] Groen, E. C., Seyff, N., Ali, R., Dalpiaz, F., Doerr, J., Guzman, E., ... & Stade, M. (2017). The crowd in requirements engineering: The landscape and challenges. IEEE software, 34(2), 44-52.

[21] M. Almaliki, C. Ncube, and R. Ali, "Adaptive Software-Based Feedback Acquisition: A Persona-Based Design," Proc. IEEE 9th Int'l Conf. Research Challenges in Information Science (RCIS 15), 2015, pp. 100–111.

[22] Dragovic, N., Madrazo Azpiazu, I., Pera, M.S.: From recommendation to curation: When the system becomes your personal docent (2018)

[23] Barria-Pineda, J., Akhuseyinoglu, K., Brusilovsky, P.: Explaining needbased educational recommendations using interactive open learner models. In: Adjunct Publication of the 27th Conference on User Modeling, Adaptation and Personalization. pp. 273{277. UMAP'19 Adjunct, ACM, New York, NY, USA (2019).

[24] Garcia, F.J.C., Robb, D.A., Liu, X., Laskov, A., Patron, P., Hastie, H.: Explainable autonomy: A study of explanation styles for building clear mental models. In: Proceedings of the 11th International Conference on Natural Language Generation. pp. 99{108 (2018)

[25] Sokol, K., Flach, P.A.: Glass-box: Explaining ai decisions with counterfactual statements through conversation with a voice-enabled virtual assistant. In: IJCAI. pp. 5868{5870 (2018)

[26] Dragovic, N., Pera, M.S.: Exploiting reviews to generate personalized and justified recommendations to guide users' selections. In: The Thirtieth International Flairs Conference (2017)

[27] Coba, L., Rook, L., Zanker, M., Symeonidis, P.: Decision making strategies differ in the presence of collaborative explanations: Two conjoint studies. In: Proceedings of the 24th International Conference on Intelligent User Interfaces. pp. 291-302. ACM (2019)

[28] Kouki, P., Schaer, J., Pujara, J., O'Donovan, J., Getoor, L.: Personalized explanations for hybrid recommender systems. In: Proceedings of the 24th International Conference on Intelligent User Interfaces. pp. 379{390. ACM (2019)

[29] https://www.enel.pe/en/sustainability/characteristics-of-a-smart-city.html

[30] https://www.iso.org/obp/ui/#iso:std:iso:ts:37151:ed-1:v1:en

[31] AENOR, UNE 178301:2015 – "Smart Cities. Open Data", 2015 https://ec.europa.eu/eip/ageing/standards/city/smart-cities/une-1783012015_en

[32] B. Risteska Stojkoska, K. Trivodaliev and D. Davcev, "Internet of Things Framework for Home Care Systems", Wireless Communications and Mobile Computing, vol. 2017, pp. 1-10, 2017.

[33] S. Sim and H. Choi, "A study on web services discovery system based on the internetof things user information", Cluster Computing, vol. 21, no. 1, pp. 1151-1160, 2017.

[34] City of Ottawa, "Samrt City 2.0: City of Ottawa Planning, Infrastructure and Economic Development", Ottawa, 2017.

[35] Degbelo A, Granell C, Trilles S, Bhattacharya D, Casteleyn S, Kray C. Opening up Smart Cities: Citizen-Centric Challenges and Opportunities from GIScience. *ISPRS International Journal of Geo-Information*. 2016; 5(2):16.

[36] Lea, Rodger, and Michael Blackstock. "Smart cities: An iot-centric approach." Proceedings of the 2014 international workshop on web intelligence and smart sensing. ACM, 2014.

[37] Cao, Q.H., Khan, I., Farahbakhsh, R., Madhusudan, G., Lee, G.M. and Crespi, N., 2016, May. A trust model for data sharing in smart cities. In Communications (ICC), 2016 IEEE International Conference on (pp. 1-7). IEEE.

[38] N. Komninos, C. Bratsas, C. Kakderi and P. Tsarchopoulos, "Smart City Ontologies: Improving the effectiveness of smart city applications", Journal of Smart Cities, vol. 1, no. 1, 2016.

[39] Vujasinovic, M., Gugliotta, A., Galizia, S. and SpA, I.N.N.O.V.A., Trust-based Discovery for Web of Things Markets.

[40] https://www.entrust.com/wp-content/uploads/2013/05/TWS_apr9.pdf

[41] Kurdi, H., Alshayban, B., Altoaimy, L. and Alsalamah, S., 2018. TrustyFeer: A Subjective Logic Trust Model for Smart City Peer-to-Peer Federated Clouds. Wireless Communications and Mobile Computing, 2018.This style is used for references

[42] V. Suryani, S. Sulistyo and W. Widyawan, "ConTrust: A Trust Model to Enhance the Privacy in Internet of Things", International Journal of Intelligent Engineering and Systems, vol. 10, no. 3, pp. 30-37, 2017.

[43] L. Atzori, A. Iera, and G. Morabito, “SIoT: Giving A Social Structure to The Internet of Things”, IEEE Communication Letter, Vol.15, No.11, pp.1193–1195, 2011.

[44] Matsuo, Y., & Yamamoto, H. (2009, April). Community gravity: measuring bidirectional effects by trust and rating on online social networks. In Proceedings of the 18th international conference on World Wide Web (pp. 751-760). ACM.

[45] https://www.techopedia.com/definition/26834/web-of-things-wot

[46] https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

[47] B. Mandler et al., “COMPOSE-A journey from the internet of things to the internet of services,” Proc. - 27th Int. Conf. Adv. Inf. Netw. Appl. Work. WAINA 2013, pp. 1217–1222, 2013.

[48] P. Anantharam, C. A. Henson, K. Thirunarayan, and A. P. Sheth, “Trust model for semantic sensor and social networks: A preliminary report,” Proc. IEEE 2010 Natl. Aerosp. Electron. Conf. NAECON 2010, no. August, pp. 1–5, 2010.

[49] F. K. Hussain, E. Chang, and T. S. Dillon, “Trust ontology for service-oriented environment,” IEEE Int. Conf. Comput. Syst. Appl. 2006, vol. 2006, no. January, pp. 320–325, 2006.

[50] M. Compton et al., “The SSN ontology of the W3C semantic sensor network incubator group,” J. Web Semant., vol. 17, no. March 2015, pp. 25–32, 2012.

[51] Tran, V. X. (2008, December). WS-QoSOnto: a QoS ontology for web services. In 2008 IEEE International Symposium on Service-Oriented System Engineering (pp. 233-238). IEEE.

[52] L. G. Anthopoulos and A. Vakali, “Urban Planning and Smart Cities : Interrelations and Reciprocities Urban Planning : Principles and Dimensions,” *Lect. Notes Comput. Sci.*, vol. 7281, no. May, pp. 178–189, 2012.

[53] S. Galizia, A. Gugliotta, and J. Domingue, “A trust based methodology for web service selection,” ICSC 2007 Int. Conf. Semant. Comput., pp. 193–200, 2007.

[54] Vujasinovic, M., Gugliotta, A., Galizia, S., & SpA, I. N. N. O. V. A. Trust-based Discovery for Web of Things Markets. https://www.w3.org/2014/02/wot/papers/vujasinovic.pdf

[55] Manduchi, R. and Kurniawan, S., 2011. Mobility-related accidents experienced by people with visual impairment. AER Journal: Research and Practice in Visual Impairment and Blindness, 4(2), pp.44-54.

[56] Guo, J., 2018. Trust-based Service Management of Internet of Things Systems and Its Applications (Doctoral dissertation, Virginia Tech).

[57] A. Marcuccetti, "From the Chalice to the Smart City: Attraction and Repulsion within Sanctified Space in the 21st Century: Projects in the New Urban Centres", CREATIVE SPACE, vol. 1, no. 2, pp. 215-229, 2014.

[58] D. Thoppil, "India’s Answer to Google Glass: The Smartshoe", WSJ, 2018. [Online]. Available: https://blogs.wsj.com/indiarealtime/2014/07/24/indias-answer-to-google-glass-the-smartshoe/. [Accessed: 21- Nov- 2018].