Leverage a Trust Service Platform for Data Usage Control in Smart City

Nguyen B. Truong*, Quyet H. Cao†, Tai-Won Um‡, Gyu Myoung Lee*
* Department of Computer Science, Liverpool John Moores University, Liverpool, L3 3AF, UK
Email: {n.b.truong@2015., g.m.lee@}ljmu.ac.uk
†Orange Labs, France
Email: quyet.caohuu@orange.com
‡Hyper-Connected Communications Labs, ETRI, Korea
Email: twum@etri.re.kr

***Abstract*—In the Internet of Thing, data is almost collected, aggregated and analyzed without human intervention by machine-to-machine communications resulting in raising serious challenges on access control. Particularly in Smart City ecosystems in which multi-modal data comes from heterogeneous sources, data owners cannot imagine how their data is used to extract sensitive information. Thus, there is a critical need for novel access control methods that minimize privacy risks while increase ability of personalized access control. Our solution is to build a trust-based usage control mechanism called TUCON that enables stakeholders to set access control policies based on their trust relationships with data consumers. In this study, we introduce two novel paradigms integrated in the Smart City shared platform: a Trust Service Platform and a Data Usage Control, then bring them together to establish the new mechanism. The conceptual model, the architecture, the formalization, and the practical development of TUCON is described in detail. We also show the roles and the interactions of TUCON components in the Smart City platform. Our contributions lie in a new trust model with a trust computation procedure based on semantic web technologies, a novel trust-based usage control conceptual model including a formalization, a practical expression and an architecture for Smart City systems. We believe this study provides better understanding on both trust and usage control in the Internet of Things and opens several important research directions in the future.**

***Index Terms*—Trust; Usage Control; Trust-based Usage Control; TUCON; Smart City; Trust Metric; Ontology**

I. Introduction

In recent years, we have been witnessing an important network paradigm the Internet of Things (IoT) which has imposed various research areas in many types of network environments. In IoT infrastructure, billions of electronic objects are connected ranging from small and low computation capability devices such as Radio Frequency Identification tags (RFIDs) to complex ones such as smartphones, smart appliances and smart vehicles. It is expected there will be more than 50 billion connected devices by 2020, approximately 6.58 devices per person on our planet [1]. The increases in quantity and connectivity result in rocketing flow of data. In IoT, most of data is collected, aggregated and mined without human intervention by machine-to-machine (M2M) communications that could lead to difficulties in complying privacy and security. Dangerously, a great portion of data owners are not aware of how their data is used. Particularly, in an environment like Smart City in which multi-modal information coming from heterogeneous sources such as location, traffic, weather, gasoline and electronic usages [2], data can be aggregated and analyzed by malicious participants to infer private information. Moreover, stakeholders also have less opportunity to learn about data-usage practices. These reasons will aggravate problems on data privacy and data sharing in Smart City. However, in order to reach full potential of intelligent and complex services, sharing data among various kinds of resources is a must. Thus, a new access control model to cope with the emerging requirements in Smart City ecosystems is an urgent need.

Our previous studies have proposed a conceptual model and a handling mechanism for data access control in Smart City based on Usage Control (UCON) in which stakeholders can put their preferences in forms of constrains and obligations on data usage [3] [4]. 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 that only institutional actors are permitted to access data in detail whereas commercial operators are permitted only statistical data on a weekly basis. This is because the data owner thinks that institutional operators are securer than commercial actors. We believe that stakeholders only share data if they trust participants regardless the type of actors. The success of any data sharing platform depends on the compliance on data protection regulations and, beyond legal obligations, on the 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 that data is only permitted to access and obligate by trusted sources. TUCON offers several benefits such as a policy enforcement that can be based on attributes of stakeholders and consumers, on obligation actions, and on trust relationships. It offers data abstraction and data monetization features, and also offers the on-the-go usage control decision that adapts with environment changes. The main contributions in this paper are following: (i) a novel trust service platform including a trust model, a system architecture, and a trust computation procedure. (ii) TUCON: a novel usage control conceptual model and architecture that considers three basic UCON factors: authorizations, obligations and conditions regarding to the trust platform. (iii) We provide formalization and prototype for the both trust service platform and TUCON including data abstraction, data annotation, semantic creation, and reasoning mechanism.

The rest of the paper is organized as follows. Section II provides background and related work on trust and usage control. Section III introduces the proposed trust model, the trust architecture, the trust computation procedure, and the practical development of the trust service platform. Section IV is dedicated to characterize TUCON including the conceptual model and the system architecture. Section V focuses on the practical expression and the prototype implementation of TUCON. We conclude our work and outline research directions in the last section.

II. Background and Related Work

A. Trust in IoT

Trust plays an important role in supporting both people and services to overcome perception of uncertainty and risk when making a decision. Trust interplays among humans, social sciences and computer science, affected by both objective factors (direct information) and subjective factors (third-party information) from physical properties to social relations [5]. In this regard, trust is a computational value depicted by relationships among a trustor, a trustee and other entities, described in a specific context, measured by Trust Metrics (TMs); and evaluated by a trust computation mechanism. In IoT, the trustor and the trustee can be human or machine, and the context is expressed as a service in a specific environment.

Our previous research has investigated the trust relationship between users and vehicles in a context considering Car Sharing service in Smart City ecosystems [6]. Trust has been accepted as one of the key factors for enhancing user privacy and system security, and for establishing seamless connectivity and reliable services. Recently, many research groups have been intensively working on trust-related areas in various environments from peer to peer (P2P) to IoT, varying in many applications from access control [7] to e-commerce [8] [9].

B. Usage Control

UCON is a new access control model initially proposed by Sandhu and Park [10] with a purpose of being addressed to emerging digital environments that can apply in various access control situations. UCON enables two advanced features to cope with dynamic networking environment: (i) the mutability of attributes, and (ii) the continuity of an access decision. Basically, UCON keeps track of changes of attributes and policies when the access is in progress, results in being able to change permission decisions. Then an authorization system revokes granted rights or terminates resource usages accordingly. The permission decisions are determined based on three factors called Authorizations, Obligations and Conditions. Authorizations are predicates over subjects (data consumers) and/or objects (stakeholders, data) attributes; put constrains on them to judge; and then grant the subjects a certain right on the objects. Obligations is a novel component in UCON model for examining the accomplishment of compulsory tasks that subjects have being done to objects before, during and after the access period. Conditions are constrains from environment attributes, not related to both subjects and objects but affect the usage decision process [11].

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. It has been widely accepted to be a prospective access control model for dynamic and open networking systems like Smart City.

C. Related Work

There are a large amount of research literature that leverages UCON for data sharing in some environments such as Social Network, Cloud Computing, IoT and Smart City. UCON features and challenges have been well studied in a survey conducted by A. Lazouski and his colleagues in [12]. Authors in [11] have extended traditional access control models for providing obligations and conditions when accessing enterprise resources, forming a simple usage control mechanism. An accountability model with an architecture have been proposed in [13], allowing participants to explore consequences of different usage control policies. A privacy model has been proposed in [14] in which semantic web technologies are utilized for supplying a privacy model and for offering users to impose their preferences and control over data in Smart Grid environment. We have continued our previous studies on data usage control [3] [4] by integrating the trust platform introduced in [6]. We believe TUCON will open several approaches for trust-based usage control model in IoT ecosystems.

III. Trust Service Platform

The trust platform cooperates with services and works as an underlying service (Trust as a Service - TaaS) to offer securer transactions and better quality of service (QoS) and experience (QoE).

A. RRK Trust Model

Despite a large amount of trust-related research, a standardization of trust model is still under investigation [15]. We follow a conceptual trust model described in [6] as follows:

- Trust is based on TMs, each TM is generally defined as the measurement of an aspect of trust.
- Each TM is calculated based on Technical Attributes (TAs). TAs are information that can be measured or extracted from data in networking environments such as Smart City systems.

In social science, people base on three sources of information to judge trust: public evidences (as reputation), opinions from surroundings (as recommendation), and their own understandings (as knowledge). We believe this process of trust evaluation can be applied for IoT system. Based on the conceptual model, a trust model called RRK is proposed comprised of Reputation, Recommendation, and Knowledge as three TMs. Each TM is derived from other sub-TMs or TAs that represent for trust aspects in Social-Cyber-Physical (SCP) world (Fig. 1).

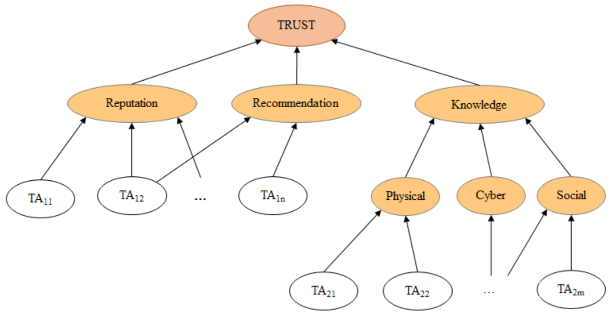

Fig. 1: The proposed RRK Trust Model

There are two methods to derive TMs from TAs and the trust value from TMs. The first method uses mathematical models such as weighted sum, Bayesian neutron networks [16], heuristic algorithms [17] or Google PageRank-like algorithms [9] for computing some sorts of TMs and TAs such as Recommendation and Reputation. The second method uses inference engines for inferring trust-related knowledge from a knowledge base to evaluate some TAs or relative trust values (i.e "*level of trust*").

B. Trust Computation System

To judge trust, sufficient data about the trustor, the trustee and the trust context needs to be collected, annotated, aggregated, and processed for creating a set of semantic information, which is a part of the trust knowledge base. The rest of the knowledge base are rules acquired by conducting a knowledge acquisition mechanism. The trust knowledge base is the input of an inference engine to reason the trust value. And based on this value, access control decisions are made accordingly. The processes to obtain the trust value are illustrated in Fig. 2.

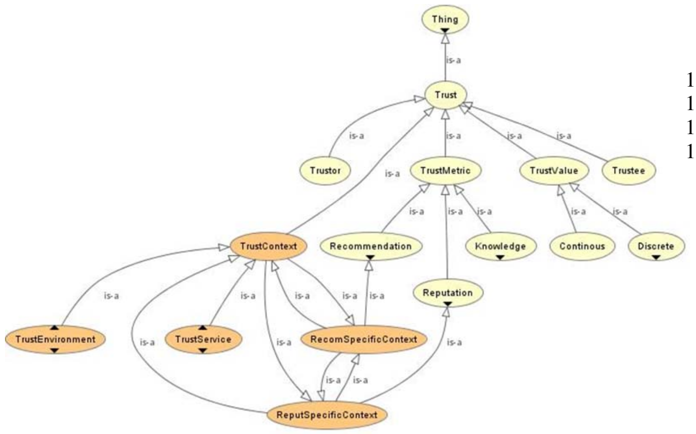

Fig. 2: The processes of the Trust Computation procedure

1) From Data to Semantic Information: Trust-related data is collected from various sorts of sources in Smart City. For example temperature, time, location are from physical objects like sensors and devices; up-time, bandwidth, packet delivery rate are from networking components in cyber-space; and relationships and exchanged information are from social media like Twitter and Facebook in social-space. The integration of SCP data enables the incorporation of situation and context-awareness, thus enabling intelligent autonomous applications and services [18]. This leads to a need for a data integration and annotation framework associated with a data model and a knowledge representation. The framework is also required for enhancing semantic interoperability for handling semantic information. State-of-the-art semantic web technologies could be used for trust modeling, data integration, and data query. For example, ontology[1] is used to represent trust and TUCON domain-specific models. Fig. 3 shows the upper ontology for RRK used in our implementation.

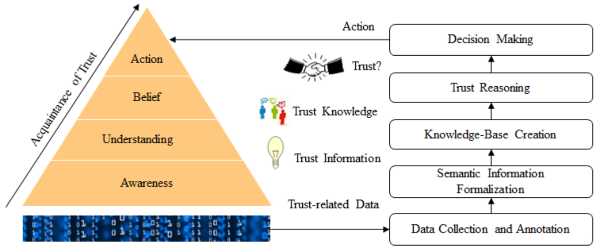

Fig. 3: The RRK Trust Model is represented in form of ontology (Trust Upper Ontology)

Based on the trust ontologies, data is annotated accordingly using RDF schema (RDFS)[2] as meta-data and semantic information (Listing1). Note that only interested information is captured in accordance with the ontologies.

```
rrk:knowledge_001 a rrk:Knowledge,
    owl:NamedIndividual;
        rrk:hasValue "Medium"^^xsd:string;
        rrk:hasPhysical rrk:physical_001;
        rrk:hasCyber rrk:cyber_001;
        rrk:hasSocial rrk:social_001.
rrk:reputation_001 a rrk:Reputation,
    owl:NamedIndividual;
        rrk:hasValue "High"^^xsd:string;
        rrk:hasCalculatedValue 0.15.
rrk:recommendation_001 a rrk:Recommendation,
    owl:NamedIndividual;
        rrk:hasValue "Medium"^^xsd:string;
        rrk:hasCalculatedValue 0.45.
rrk:trust_001 a rrk:Trust, owl:NamedIndividual;
        rrk:hasValue "High"^^xsd:string.
```

Listing 1: RDFS data for an individual of RRK Trust Model.

The data can be published using Linked Data so that it is interlinked and enabled to semantic queries [19]. Several RDF-query languages such as SPARQL [20], an SQL-like language, can be used to query the triple store.

2) From Semantic Information to Trust Knowledge Base: The trust knowledge base contains structured and unstructured information represented in a machine-interpretable language in

[1] Web Ontology Language by W3C: https://www.w3.org/TR/owl2-overview

[2] RDF 1.1 Primer, W3C: https://www.w3.org/TR/rdf11-primer

order for reasoning trust value 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 logic among concepts contained in the facts (procedural knowledge) [21]. In the trust prototype, we use a knowledge representation formalism combining both rule-based language and ontology for supplying reasoning capabilities. Specifically, the semantic information extracted in the first process is converted into facts in form of Description Logics [22]. The rules can be monotonic or non-monotonic to express knowledge on ontologies such as classes, sub-classes, instances and relations. The rules are the most important part of the knowledge base which interpret meanings and describe relationships of the concepts in the facts. Depending on rule-based languages being used, rules are encoded in different syntaxes such as Jena[3] and Pellet[4].

The process to create rules for the knowledge base is called knowledge acquisition, a part of knowledge engineering. It is a complicated process that acquires knowledge from many resources such as user preferences, domain experts, documents, Internet resources, etc., using various methods such as interview with human; data mining and machine learning over data and Internet resources [23]. In the prototype, for simplicity, the rules are predefined. For instance, a Jena rule for evaluating Knowledge TM is as below:

```
knowledge_001_rule1:
(rrk:physical_001 rrk:hasValue "high"),
(rrk:cyber_001 rrk:hasValue "low"^^),
(rrk:social_001 rrk:hasValue "medium")
-> (rrk:knowledge_001 rrk:hasValue "medium")
```

The meaning of the rule is that: if values of the three Physical, Cyber, Social sub-TMs are ”high”, ”low”, and ”medium”, respectively, then the value of the Knowledge TM is ”medium”

3) Trust Reasoning Mechanism: Based on facts and rules, inference engines can draw new knowledge that we are interested, i.e ”*level of trust*”. In this study, the trust value is simplicity defined in three levels: low, medium and high meaning as distrust, normal and trust, respectively. The reasoner takes the trust knowledge base as its input and infers new knowledge as new facts, resulting in additional rules in the knowledge base being triggered; then new facts could be created. This process would iterate until a goal has been reached or until no rules can be matched. We use Apache Jena framework that supports various types of integrated inference engines with forward chaining, tabled backward chaining, and hybrid reasoning strategies for our demonstration.

C. Trust Service Platform Architecture in Smart City

The trust platform architecture is called Trust Analysis and Management Platform (TAMP) that comprises of four components namely Reputation System, Trust Agent, Trust Broker and Trust Engine (Fig.4). It is introduced and described in detail in our previous work [6]. In the section IV, we will describe how the components of TAMP and TUCON are incorporated in the Smart City shared platform.

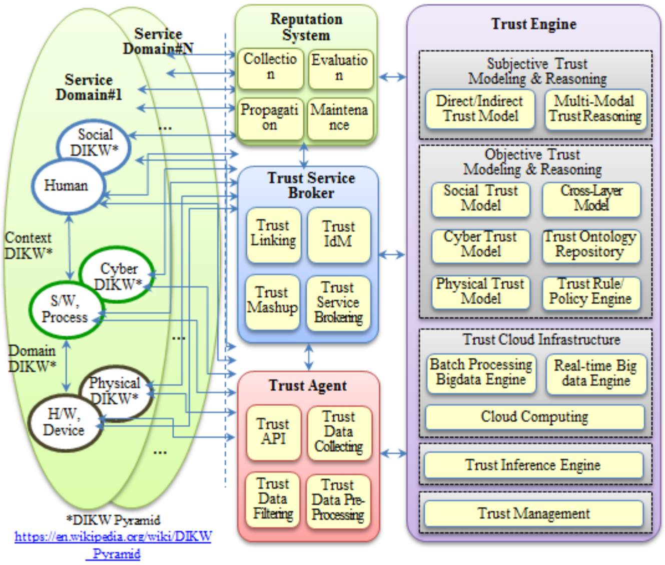

Fig. 4: Components and Interactions in the Trust Service Platform

IV. Trust-based Usage Control Mechanism

A. TUCON Conceptual Model

The initial step in the design of any UCON mechanism is to identify the objects to be protected and the subjects that request to access and perform actions on objects. Actions are obligations describing how the objects are exploited by the subjects. It is needed to define Access Rights associated with each of the Obligations; and define the Authorizations that predicate the access rights based on attributes (ATT(O)), subjects attributes (ATT(S)) and the environment attributes (as Conditions). In TUCON, the objects are dataset owned by stakeholders, the subjects are data consumers, the conditions are the trust relationship between data owners and data consumers (Fig. 5). The details of this model is clearly described in section V.

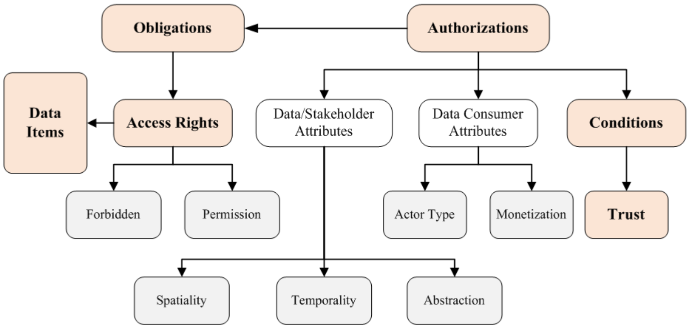

Fig. 5: TUCON conceptual model.

B. TUCON System Architecture

The architecture is built associated with the 3-layered Smart City shared platform proposed in [24] [25]. The three layers

[3] https://jena.apache.org
[4] https://github.com/complexible/pellet

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 that are 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) works as an interface between application and PLA. The Ontology Manager (OM) is also introduced for data annotation and for supporting Wireless Sensor Networks (WSN) services using domain ontologies such as Semantic Sensor Networks (SSN) in [26].

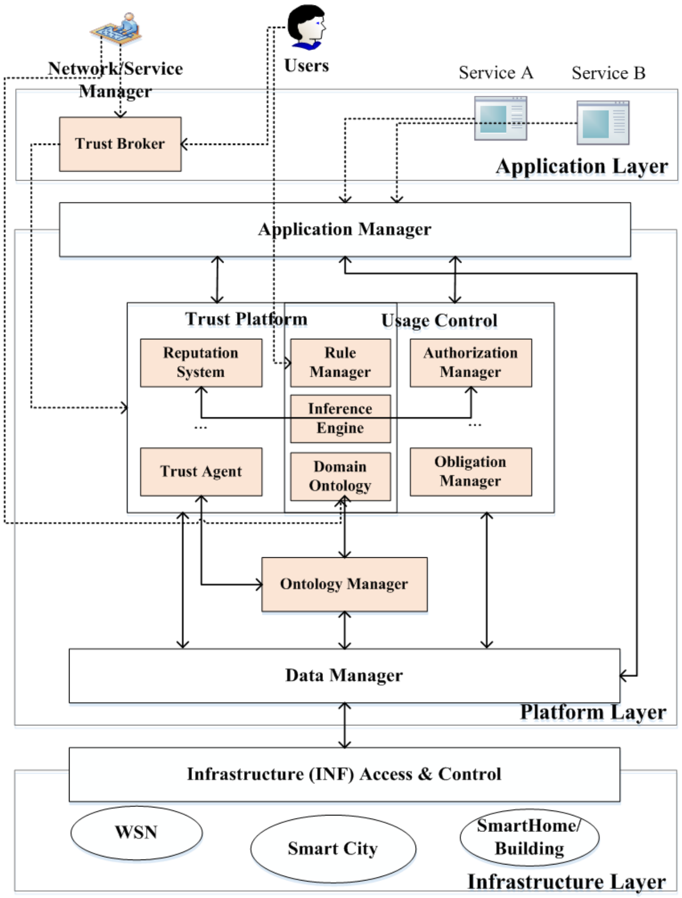

Fig. 6: The proposed TUCON architecture in the smart city shared platform

The TUCON architecture is developed by incorporating TAMP with UCON components into the 3-layered shared platform. As illustrated in Fig. 6, the 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 as well as authorization policies in TUCON. Note that the rules describe the relationships among classes and individuals in the ontologies, thus, incurs interactions among RM, DO and OM. RM directly interacts with Users for acquiring user preferences in the form of rules (in case of TUCON). RM also interacts with Trust Brokers for the user preferences (in case of TAMP).
- IE implements some reasoners for inferring new facts and trust values in TAMP; and for inferring access rights in TUCON. TUCON and 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 (DL) 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.

V. PRACTICAL EXPRESSION AND PROTOTYPE

A. DataItems

A Data Item is an individual of Context Element container proposed in the NGSI 9/10 Information Model[5] that is used to exchange information about an entity, including entity ID, context attributes, related attribute domains, and meta-data for all of the attributes of the given domain. DataItem is formally defined in XML DTD syntax as in Listing 2.

```
<!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)>
...
]>
```

Listing 2: XML DTD Definition of Data Item

B. Authorizations

TUCON policies represent constrains based on object attributes, subject attributes and conditions. Authorizations optionally contains 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 describes purposes of using data such as selling, training, or providing customer supports. (iii) Conditions: trust values between data owner (trustor) and data consumers (trustee). Authorization XML DTD definition is in Listing 3.

```
<!DOCTYPE TUCON[
  <!ELEMENT  Authorization(ATT_O*,  ATT_S*,
    Condition*)>
  <!ELEMENT  ATT_O( Spatiality*, Temporality*,
    Abstraction*)>
  <!ELEMENT  ATT_S( Actor *, Monetization *)>
  <!ELEMENT  Condition(Trust *)>
```

[5] https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/NGSI-9/NGSI-10 information model

```
  <!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?)
    >
  ...
  ]>
```

Listing 3: XML DTD Definition of Authorization

C. Obligations

This is a set of actions on DataItems such as Full Access, Partly Access, Dissemination, Storage, and Analysis. Obligations actions are associated to Data Monetization. For instance, if a data consumer requests for selling data, then Obligation action should be Dissemination; or if the data consumer requests for statistical training, then Obligation action should be Partly Access with constrains Temporality = Weekly & Abstraction = Statistical. XML DTD definition of Obligations is in Listing 4.

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

Listing 4: XML DTD Definition of Obligations

D. Access Rights

Decisions are in accordance with Obligations actions and Authorization values. We simply define as Permission and Forbidden reflecting whether DataItems are allowed to "*share*" or not. The word "*share*" is more specifically understood in the TUCON context as: "*allow to conduct appropriate obligation actions*". AccessRights is defined in XML DTD syntax in Listing 5.

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

Listing 5: XML DTD Definition of Access Right

E. TUCON Formalization and Expression

The formalization is based on DL, a non-monotonic formalism with normative conflicts-solving ability and low computational complexity [27]. Particularly, an extension of DL 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 [28] [29]. We take several examples to show how DL is applied:

1) Facts: The Facts in DL represent the ATT(O), ATT(S) and Condition (trust values). For example, two institutional organizations (IO1 and IO2) with the trust levels as "High" and "Low", respectively, are represented as below:

```
F1TUCON(IO1): {ActorScope(Institutional)}
F2TUCON(IO1): {TrustScope(High)}
F1TUCON(IO2): {ActorScope(Institutional)}
F2TUCON(IO2): {TrustScope(Low)}
```

2) Rules and Superiority Relations: All constrains among stakeholders, data, actors, conditions and AccessRight are represented in DL rules. There are three different rules types that carry 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 conclusion whereas defeater rules are only used to prevent from making conclusions. Superiority relations of rules are used to set the priority among these rules and to resolve conflicts. The following is an example of defeasible rules and superiority relations of the two institutional actors IO1 and IO2:

```
R1TUCON(X): {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 shorts for Obligations action, and is a modal operator of the DL extension. The example is explained as following: by default, any institutional organization is allowed to conduct OB on data at spatial street level. However, this policy can be overruled when considering trust relationship between the actor and the data owner. For example, if trust value is high, then the actor can access all spatial level of data (actor IO1) or if trust value is low, then only zone level of data is permitted.

3) DL Inference Engine and TUCON request: An example of a consumer X that requests for data with Obligation action OB is expressed as following:

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

A DL inference engine is used to get conclusion that whether RreqTUCON is defeasible proven in the DL theory or not. The inference algorithm is based on DL Proof Theory mentioned in [27]. Several DL reasoners can be applied and we choose Spindle[6] for the demonstration. The conclusion is as following:

```
# Conclusions
===================
-D Rreq.TUCON(X[OB])
-d Rreq.TUCON(X[OB])
```

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

showing that the Rreq.TUCON(X[OB]) request is Defeasible Provable in the DL theory. Thus, the data consumer satisfies all authorization policies to obligate the action OB on the stakeholders data, the AccessRight now is Permission. DL formalism is suitable for usage control since facts, rules are defeasible that can be overruled by supplying more facts, rules, and superior relations, resulting in enabling the ability of continuity of access decisions in TUCON.

VI. CONCLUSION AND FUTURE WORK

We have introduced the TUCON usage control mechanism that leverages a trust service platform to provide securer access control over data on Smart City based on trust relationships between data owners and data consumers. Firstly, we present the trust service platform TAMP in accordance with the RRK trust model, the trust platform architecture and the trust formalization. The trust computation implementation based on semantic-web technologies is also prototyped. Secondly, we introduce the TUCON conceptual model and architecture considering trust components in the three-layered Smart City shared platform. Finally, the practical expression and prototype for TUCON components are clearly characterized using DL.

There are two main research directions that could be taken to fulfill the TUCON mechanism. The first direction is the improvement of the TAMP by developing an automated intelligent rules creation for the trust knowledge base instead of being predefined. This can be done by using machine learning techniques for rules pattern recognitions. A verification mechanism is also needed to investigate to check the quality of the knowledge base such as consistency and redundancy. The second direction is to strengthen TUCON by improving usage control model, formal model, architecture and enforcement mechanisms as well as enhancing mutuality of attributes and continuity of access decisions.

ACKNOWLEDGMENT

This research was supported by ICT R&D program of MSIP/IITP [R0190-15-2027, Development of TII (Trusted Information Infrastructure) S/W Framework for Realizing Trustworthy IoT Eco-system] and EU funded Horizon 2020 Wise-IoT project [The EC Grant Agreement No. 723156, Worldwide Interoperability for Semantics IoT].

REFERENCES

[1] D. Evans, "The internet of things how the next evolution of the internet is changing everything," 2012.

[2] P. Barnaghi, M. Bermudez-Edo, and R. Tönjes, "Challenges for quality of data in smart cities," *Journal of Data and Information Quality (JDIQ)*, vol. 6, no. 2, p. 6, 2015.

[3] Q. H. Cao, G. Madhusudan, R. Farahbakhsh, and N. Crespi, "Usage control for data handling in smart cities," in *2015 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2015, pp. 1–6.

[4] 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.

[5] B. Alcalde, E. Dubois, S. Mauw, N. Mayer, and S. Radomirović, "Towards a decision model based on trust and security risk management," in *Australasian Conference on Information Security*. Australian Computer Society, Inc., 2009, pp. 61–70.

[6] N. B. Truong, T. Won, and G. Lee, "A reputation and knowledge based trust service platform for trustworthy social internet of things," in *Innovations in Clouds, Internet and Networks (ICIN)*. IEEE, 2016.

[7] 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)*. IEEE, 2013, pp. 1–5.

[8] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision support systems*, vol. 43, no. 2, pp. 618–644, 2007.

[9] S. Brin and L. Page, "Reprint of: The anatomy of a large-scale hypertextual web search engine," *Computer networks*, vol. 56, no. 18, pp. 3825–3833, 2012.

[10] J. Park and R. Sandhu, "Towards usage control models: beyond traditional access control," in *ACM symposium on Access control models and technologies*. ACM, 2002, pp. 57–64.

[11] ——, "The ucon abc usage control model," *ACM Transactions on Information and System Security (TISSEC)*, vol. 7, pp. 128–174, 2004.

[12] A. Lazouski, F. Martinelli, and P. Mori, "Usage control in computer security: A survey," *Computer Science Review*, vol. 4, pp. 81–99, 2010.

[13] J. Pato, S. Paradesi, I. Jacobi, F. Shih, and S. Wang, "Aintno: Demonstration of information accountability on the web," in *Privacy, Security, Risk and Trust (PASSAT) and IEEE Third Inernational Conference on Social Computing (SocialCom)*. IEEE, 2011, pp. 1072–1080.

[14] S. Speiser, A. Wagner, O. Raabe, and A. Harth, "Web technologies and privacy policies for the smart grid," in *39th Conference of IEEE Industrial Electronics Society (IECON)*. IEEE, 2013, pp. 4809–4814.

[15] Y. L. Sun, W. Yu, Z. Han, and K. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *Selected Areas in Communications, IEEE Journal on*, vol. 24, no. 2, pp. 305–317, 2006.

[16] F. Bao, I.-R. Chen, and J. Guo, "Scalable, adaptive and survivable trust management for community of interest based internet of things systems," in *Autonomous Decentralized Systems (ISADS)*. IEEE, 2013, pp. 1–7.

[17] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation systems," *Communications of the ACM*, vol. 43, no. 12, pp. 45–48, 2000.

[18] A. Sheth, P. Anantharam, and C. Henson, "Physical-cyber-social computing: An early 21st century approach," *Intelligent Systems, IEEE*, vol. 28, no. 1, pp. 78–82, 2013.

[19] C. Bizer, T. Heath, and T. Berners-Lee, "Linked data-the story so far," *Semantic Services, Interoperability and Web Applications: Emerging Concepts*, pp. 205–227, 2009.

[20] O. Hartig, C. Bizer, and J.-C. Freytag, "Executing sparql queries over the web of linked data," in *International Semantic Web Conference*. Springer, 2009, pp. 293–309.

[21] S. Russell, P. Norvig, and A. Intelligence, "Knowledge and reasoning: A modern approach," *Artificial Intelligence. Prentice-Hall, Egnlewood Cliffs*, vol. 25, p. 27, 1995.

[22] F. Baader, *The description logic handbook: Theory, implementation and applications*. Cambridge university press, 2003.

[23] S. L. Kendal and M. Creen, *An introduction to knowledge engineering*. Springer, 2007.

[24] I. Khan, F. Belqasmi, R. Glitho, N. Crespi, M. Morrow, and P. Polakos, "Wireless sensor network virtualization: early architecture and research perspectives," *Network, IEEE*, vol. 29, no. 3, pp. 104–112, 2015.

[25] I. Khan, R. Jafrin, F. Z. Errounda, R. Glitho, N. Crespi, M. Morrow, and P. Polakos, "A data annotation architecture for semantic applications in virtualized wireless sensor networks," in *International Symposium on Integrated Network Management (IM)*. IEEE, 2015, pp. 27–35.

[26] M. Compton, P. Barnaghi, C. Bermudez, A. Herzog *et al.*, "The ssn ontology of the w3c semantic sensor network incubator group," *Web Semantics: Science, Services and Agents on the World Wide Web*, vol. 17, pp. 25–32, 2012.

[27] D. Nute, "Defeasible logic," in *Handbook of logic in artificial intelligence and logic programming*. Citeseer, 1994.

[28] E. Kontopoulos, N. Bassiliades, G. Governatori, and G. Antoniou, "A modal defeasible reasoner of deontic logic for the semantic web," *International Journal on Semantic Web and Information Systems (IJSWIS)*, vol. 7, no. 1, pp. 18–43, 2011.

[29] G. Antoniou, N. Dimaresis, and G. Governatori, "A modal and deontic defeasible reasoning system for modelling policies and multi-agent systems," *Expert Systems with Applications*, vol. 36, no. 2, pp. 4125–4134, 2009.