Journal of Ubiquitous Systems & Pervasive Networks
Volume 6, No. 2 (2015) pp. 01-10

PRIVACY AWARE SMART OBJECTS IN INTERNET OF THINGS

Afshan Samani[a] , **Hamada H.Ghenniwa** [a] *, **Abdulmutalib Wahaishi** [b]

[a] Electrical and Computer Engineering, Western University, London, Ontario, Canada
[b] *College of Information Technology, United Arab Emirates University, Al Ain, UAE*

Abstract

The Internet of Things (IoT) is becoming the new computation environment in which the “things” such as software and information services, devices, equipment and sensors are interconnected and have the ability to share and exchange data accordingly. To adequately treat IoT as computation environment, IoT need to be modelled as a computation platform.

However, due to the exponential adoption of IoT application by people and organizations within all aspects of their day-to-day matters, users’ requirements for privacy protection are becoming essential and complex beyond the traditional approaches. This requires a formal treatment of “privacy” as a fundamental computation concept.

In this work, we model IoT as Cooperative Distributed Systems (CDS) in which entities are autonomous and self-interested. The fundamental computation entities in CDS are viewed as Smart Object (SOs) and modelled as Collaborative Intelligent Rational (CIR) Agents. The SOs are hence extended to accommodate and protect privacy in open environments such as the IoT. Privacy protection is captured as a form of “sensitive information” management at the interaction level. The feasibility of the proposed models has been demonstrated by developing an agent-based CDS platform for privacy-aware smart objects using JIAC framework.

Keywords: *Privacy, IoT, Smart Object, Cooperative Distributed Systems (CDS)*

1. Introduction

The Internet of Things is becoming the new computation environment with interconnection of “things” such as software and information services, devices, equipment and sensors that are able to communicate with each other via the Internet. Incorporation of social networks and ubiquitous computing technologies in IoT enables individuals and groups of people to engage seamlessly with the environment [1]. To adequately treat IoT as computation environment and address the characteristics of this environment, IoT need to be modelled as a computation platform. In this work, we propose modelling IoT as Cooperative Distributed Systems (CDS) in which entities are autonomous, self-interested and are expected to have some degree of authority in sharing their information and capabilities [8]. As “things” in IoT have the capability to perform various computations and engage in many communications and decision-making processes, these entities are viewed as “Smart Objects” that are modelled as Coordinated Intelligent Rational (CIR) agent, and thus enable IoT to be treated as a computation platform.

In contrary of the growth and advancement that is envisioned for IoT, it comes with various challenges. The comfort that is experienced through the innovative technologies in IoT was with the expenses of privacy [2], [3]. For instance, a message is post in a customer Facebook page after they show up at a store and the video sensor collects their picture. Face detection services identify their name and RFID tags locate the store. Through this, not only the people are tracked but also their location is shared with other people in their network. In spite of the employment of privacy mechanism [19] such as anonymization [4], [20], utility tradeoffs [5], [22], proxy based approaches [6], and establishing more profound and strong legal restrictions on data extraction and identification, privacy still is a major challenge in IoT. Some of these models presume a particular setting for environments [4]. Some others are not addressing the preferences of entities and they are based on information gain only [5]. Also, some privacy protection models adhere to strong assumption of having trusted “things” in the environment [6], [7].

Privacy is the concern of computational systems that have decentralized computation. To deal with this, privacy has to be captured as a computation concept and integral part of the

* Corresponding author. Tel.: +15196612111
E-mail: asamani5@uwo.ca

DOI: 10.5383/JUSPN.06.02.001

computation platform. This requires treating privacy as a mathematical object and incorporating it as a quality factor for the solutions that are computed. The efforts we made in analysing privacy in CDS resulted in developing a model that represents privacy as a computational concept and is used as an analytical tool to evaluate the state of privacy in various settings of interactions in CDS. We propose an interaction-based privacy protection framework through which "things" in IoT rely on privacy protection that is captured at the computation platform. In this work, we have captured privacy as a computation concept and extended the computation entity model (CIR-Agent) to include privacy at the interaction level through which the solutions that are achieved will inherit privacy by nature.

The rest of the paper is structured as follows: Section 2 explicates on IoT as a computation environment. Section 3, depicts the applicability of modelling the IoT environment as CDS. Section 4 provides the view on privacy in decentralized environment. Section 5 presents a model for privacy in CDS model. Section 6 elaborates on a framework for managing privacy protection at interaction level for CDS-based IoT. In Section 7, the architecture and implementation model of privacy aware Smart object is presented. Subsequently, the feasibility of this model and implementation challenges of privacy-aware Smart Object has been discussed in section 8. The work is concluded in section 9.

2. Internet of Things: New Computation Environment

Computation history is replete with changes in how people regard, use and interact with computers. With the recent evolution of computation from the colossal machines to the ever-present digital era that is characterized by technologies such as nanotechnologies, quantum computing, cloud-based computing, mobile computing and the new area of computation known as Internet-of-Things (IoT), a great paradigm shift through which many technological services have become part of nearly every human activity. Primitively, IoT was coined in AUTO-ID Center at Massachusetts Institute of Technology (MIT) while designing cross-company RFID infrastructure. Thereafter, it evolved with being a platform for making computation firmly ubiquitous [25]. In 1966, it was envisioned by Karl Steinbuch that in few decades "computers will inter-woven into almost every industrial products". With the estimation of having 50 billion internet-connected devices and having 5 to 10 internet-based handsets for each PC in 2020, this vision has realized and predicted to become more pervasive in new future [26]. The growth of IoT and the anticipated feature advancements has disrupted many industries such as health [27] and automobile [28]. Emerging of wearable devices, ultramobiles and electric cars has introduced IoT to other industries through which IoT is the computation environment for applications associated to each industry. Each of the "things" in IoT is an entity with communication and computation capabilities [29] that enables IoT environment to become the computation platform for various applications. Capturing IoT as a computation platform necessitates modelling the environment through which its characteristics can be adequately modelled and analysed. Such model currently is lacking. In the following section, we propose modelling IoT environment using Cooperative Distributed Systems (CDS) that enables addressing IoT challenges and characteristics as computational concepts.

3. IoT: Characteristics and Model

In this work, the fundamental element of IoT are "things" that are equipped with digital computational processes and Internet-based communication capabilities. "things" are capable of exchanging information with other "things" in attempt to cooperate to achieve individual and collective goals. "things" goals may be beyond their capabilities to achieve for which they may coordinate with others to achieve the goals. IoT naturally evolved as an open environment in which entities with varied types of designs, business objectives and behaviours can join the environment and leave it at any time. This adequately leads to model IoT as a CDS in which entities are viewed as Smart Objects (SO) that are capable of coordinating their activities with others to achieve individual or collective goals. SO can be autonomous and self-interested computation objects with incomplete knowledge. In this context, SO represent "things" that are capable of sharing information and making decision based on self-interested objectives.

Smart Objects (SOs) are modelled as CIR-agents [8] that posses knowledge and capabilities. Figure 1 shows the logical architecture of a CIR-agent. Knowledge in this model conveys all information regarding self-model, other SOs model and domain actions. The domain actions include the information regarding operations that the SO possesses. The problem solving component outlines the role of a specific SO and the relevant operations that can be applied in order to achieve goals.

The IoT is increasingly becoming integral within people's day-to-day life business entities' actions which the information might be considered as "sensitive" in relation with other SO of the environment. To provide a service, information might be exchanged and transferred to different SO within the environment for collecting and processing. This may impose privacy concern. As an example, magnet sensors enable opening doors through internet. However, for security reasons they are bound to video sensors to authorize people at the entrance. Applying the face detection programs on videos combining with the frequency of appearances of people in the house, may lead to identify members of the family including children. Using Facebook face recognition software also makes it possible to find their facebook pages and possibly the school that they are going [13], [14]. Accordingly, modelling IoT as CDS based environment allows addressing the privacy issues at CDS model. In the following, we have argued that privacy is the characteristics of the interaction of SOs which can be treated as a computation concept.

4. Privacy: Concern of Decentralized Environments

The evolution of CDS created new forms of computation that instituted the significant advances, involvement and

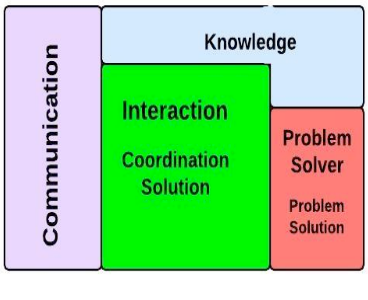


Figure 1. Logical Architecture of CIR-Agent

tremendous impacts of information technology on peoples' lives. In CDS, autonomous self-interested entities require the capabilities of others, resulting in interaction and exchange of information between these entities. It is envisioned that information is collected by many processes and devices and hence has brought increased risks regarding the concerns on one's privacy. Information about people is gathered through many service providers, stored in various infrastructures, analysed and reported for further objectives [4]. The information is manipulated towards extracting and disseminating the information to other parties or serving various interests.

The computation in distributed heterogeneous environments that are modelled as CDS such as IoT occurs during interaction between entities where the information is shared. This entails capturing privacy at the computation level [5]. This view is contrary to the traditional approaches towards privacy through which the application filters the computation solutions based on predefined rules [6], [7]. The privacy models can be classified into two main categories: rule-based approaches and architectural-based approaches [8]. Privacy solution models that evolve from rule-based approaches are typically designed for stable, low variant environments. These approaches mainly concentrate on applying rules onto information that is collected during the process of sharing. Due to the open environment assumption in many applications of CDS, the rule-based approaches [9] are not sufficient [18], [10]. The rue-based approaches in general confront with the limitation of rule designing and the results of processing information are not captured in in these approaches. Among architectural-based privacy solutions are anonymization techniques [11], [12], [13], privacy utility trade off mechanisms, [5], [14], [15], [21] social tradeoffs and proxy-based privacy protection [16]. In this context, the anonymization techniques are limited to particular settings that include a trusted information collector entity and non-continuous information dissemination processes for which it cannot be adopted by open CDS environments [17]. The work in [16] illustrates that privacy utility trade off models do not necessarily reflect the preferences that each entity might have over their privacy. The utility tradeoff mechanisms have been applied in contexts such as smart power grid in which privacy is reduced to limited access to individualized signal from the aggregated view of the collected signal [15]. These models also evolved with approaches for measuring the risk of privacy concerns. Such risk adheres to the execution of operations that causes privacy concern but it can measure the probability of the entity's information being used [23]. In all cases, the limitation of the proposed models indicates the lack of adequate privacy model for CDS.

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

5. Privacy in CDS: Concepts, Analysis and Model

The focus in this section is on analysing the main aspects of privacy concerns and concepts that are essential to develop a privacy protection framework. Sharing information among smart objects in IoT occur whenever an interaction takes place. The interaction is delivered through message-based communication. These messages convey information which may raise privacy concerns as such smart objects desire to not sharing sensitive information with others. For any given information or state of a SO, there is a boundary for exposure within which information shared is not sensitive. This suggests our definition of "privacy" as the state of exposure boundary of a smart object's information with the outside world. In CDS, IoT is modelled as a set of SO entities: $W = \{e_1, \dots, e_N\}$.

In the context of information management, entities can be modelled as operations and information. $e_i = < O_i, I_i >, 1 \le i \le N$

$I_i = \{I_{i,1}, \dots, I_{i,k}, \dots, I_{i,K}\}$, $1 \le i \le N, 1 \le k \le M$, $O_i = \{o_{i,1}, \dots, o_{i,w}, \dots, o_{i,W}\}$, $1 \le i \le N, 1 \le w \le W$

In this context, the information that flows within the boundary is considered non-sensitive but it is considered sensitive when it flows outside the exposure boundary. For instance, in smart house applications that are developed using IoT, the detailed energy consumption pattern of each room collected by sensors is communicated to the house manager application that can be running on a cellphone. However, the exposure boundary of this information does not include the power provider company. This information can be used for realizing the pattern of availability of the house holder in the house by capturing the lowest consumption times which is considered sensitive information for many house holders. Let $B_{i,k}$ be the exposure boundary that is designated by the smart object e_i for $I_{i,k}$: $B_{i,k} = \{e_{i,1}, \dots, e_{i,r}\}, 1 \le r, 1 \le N, \subset (B_{i,k}, W)$

Accordingly, sensitive information is relative to the smart object that the information is shared with. If it does not belong to the privacy exposure boundary, the information becomes sensitive. Also, sharing in the context of information privacy is the process of exchange of explicit information within the exposure boundary $B_{i,k}$.

Information can also be exhibited as implicit. "Implicit information" can be transformed to explicit by the execution of some operation (I^{x1}, I^{aux}) . Manipulation of explicit information I^{x1} by processing operations can transform the implicit information into explicit form I^{x2} through execution of the operation which is denoted as: $o(I^{x1}, I^{aux}, I^{x2})$. Operations may utilize auxiliary information I^{aux} that is not shared by the owner.

Although SO can protect their explicit sensitive information, it becomes a concern when the implicit information can be transformed into explicit sensitive information. Disseminating information also can be modelled by operations where the functionality of the operation is to transfer the information to other smart objects.

Sharing information with SOs that possess operations that can transform the corresponding implicit information to explicit is called disclosure. This indicates that by sharing non-sensitive explicit information, it can be equivalent to disclosing sensitive implicit information. Accordingly, the main concern with privacy becomes disclosure of sensitive implicit information.

One of the main challenges of privacy protection management is to cope with incomplete knowledge. In this context, it is essential for SO to attain the knowledge about operations of other SO that might share information with. It is used to identify what sensitive information can be retrieved due to the disclosure of information. To deal with this issue, we introduce "authorized" operations i.e $O_j^{i,j}$ that is a set of operations belonging to O_j where s_j has agreed on applying them on $I_{i,j}$. As an example, this can be enforced using legal agreements among web services. Ideally, these agreements include the operations that are allowed to be applied on the shared information. Dishonouring the agreement between the SO of execution of non-authorized operations is considered a form of "privacy violation".

In contrary, "Privacy protection" then can be defined as the enforcement mechanisms to prevent or to neutralize the application of non-authorized operations on shared information that is denoted as $PP\left(s_i, \left(PS(I_i)\right), O\right)$.

Typically, privacy concerns is associated with negative impacts or cost as a consequence of disclosing information that lead to the execution of non-authorized operations. Additionally, because of incomplete knowledge assumption in smart objects, the model is extended to capture the risk of occurrence of the negative impact [15].

6. Privacy Protection Framework

We propose an interaction-based privacy protection management framework for CDS. The approach can be based on two strategies: (i) restricting the non-authorized operations, and (ii) neutralizing the execution of non-authorized operations. A "perfect" protection that can prevent or neutralize all non-authorized operations might not be attainable, due to the incompleteness of the smart objects' knowledge. In this case, "quasi" protection mechanisms can be applied. For instance anonymization techniques can be applied to provide privacy protection with a certain degree of probability. The anonymization techniques are typically used for clinical and medical research collaborations [16]. However, depending on the anonymization technique, we can provide privacy protection with some level of confidence factor. Alternatively, applying rule-based mechanisms can be used to restrict limited number of non-authorized operations. Here, we introduce a measure for the degree of the "Privacy Protection Level " (PPL). PPL is a probabilistic base model describing the effectiveness of a mechanism to restrict or neutralize non-authorized operations from producing sensitive information. Consider a privacy protection mechanism μ which is defined over a space S to prevent the execution of non-authorized operation: $\mathbb{I} = PP\left(s_i, S, O_i^j(S)\right)$

For a quasi mechanism, applying a mechanism over the space of SO information may exhibit uncertainty with regards to PPL. We can model this as the conditional probability of the protecting privacy by μ given the space of I_i as: $PPL(s, I_i, \mu) = P(\mu \mid I_i)$.

Privacy protection mechanisms in both forms of perfect or quasi can occur at two levels. Firstly, protection at the operation level at which non-authorized operations can be identified. An example is rule based authorization engines. Secondly, approaches are based on applying information level protection to neutralize the execution of non-authorized operations. An example of this approach is differential privacy that attempts to distort the information by adding noise. Privacy protection mechanisms can be modelled in terms of operations O^{μ} and information I^{μ} : $\mu = < O^{\mu}, I^{\mu} >$

Privacy protection mechanism also can be categorized as "preventive" and "punishing". Preventive information-based mechanisms provide protection by manipulating information during the interaction to limit disclosing the sensitive information. The examples of these mechanisms are anonymization techniques [4] or encryption methodologies [18] applied for privacy protection. Preventive protection mechanism attempts to limit non-authorized operations from generating sensitive information. As an example, rule-based authorization engines prevent the execution of non-authorized operation in regards to the specified rules. The punishing approaches in privacy protection mechanisms are where prevention is not applicable or not sufficient. Punishing mechanisms are agreement-based between the interacting parties. The mutual agreement describes the structure of the privacy violation. It includes the non-authorized operations and punishing processes. An example is the terms and conditions that are agreed upon by the smart objects and the associated legal responsibilities. If any non-authorized operation is executed, there will be legal consequences for the faulty SO.

6.1 Interaction Based Privacy Protection

Interaction is a mechanism that SO adopt to perform coordination that deals with interdependency problems such as capability, interest, knowledge and resources. Let interaction be $< \delta, s_i, s_j, IP >$ where δ is the kind of interdependency; s_i and s_j smart objects involved in the interaction. IP is the interaction protocol acquired by smart objects. Let IP be a message-based protocol denoted by $< M, S_M >$; M is the set of messages and S_M is the sequences of messages. $M(IP$) refers to the M of IP and $S_M(IP)$ address the sequence associated to IP. In this work we focus on extending the interaction protocol with privacy protection ability.

In this context, IP can be modeled as a set of operations that collect and disseminate information, it is and denoted by $IP = < o^{IP,1}, \dots, o^{IP,k}, \dots, o^{IP,Q} >$.

Also, protection mechanism is a sequence of operations: $O^{\mu} = < o^{\mu,1}, \dots, o^{\mu,j}, \dots, o^{\mu,D} >, 1 < j < D$

The proposed framework for privacy protection extends the interaction protocol with the operations of the privacy protection mechanism. We propose three forms of extensions. Firstly, the protection mechanism operations are concatenated to the interaction protocol operations as prefixes. For instance, before the medical information collected by sensors is communicated to smart objects in a laboratory, the operations regarding anonymization and encryption are performed. The result is submitted to the operation in interaction protocol and they can deliver the anonymized information to the smart objects in the laboratory: $< o^{m,1}, \dots, o^{m,D}, o^{IP,1}, \dots, o^{m,Q} >$

Secondly, the privacy protection mechanism operations are appended to operations of the protocol such as the operations that happens by re-enforcements: $< o^{IP,1}, \dots, o^{m,Q}, o^{m,1}, \dots, o^{m,D} >$.

Privacy Protection for this interaction typically can be addressed as punishing mechanisms. For instance, reporting to monitoring entities and the subsequent discipline can be incorporated to the interaction protocol.

Thirdly, the extension is based on merging privacy protection mechanism operations with the interaction protocol operations in which the order of interaction protocol operations does not impact the soundness of the protocol. The sequence of the mechanism operations within the protocol is determined by the contained information. For instance, IaaS providers encrypt consumers storages as well as adhering to the participation of a third party for analysing anonymized consumers' information and receiving aggregated views about the consumption patterns:

$$< o^{IP,1}, \dots, o^{m,1}, \dots, o^{IP,q}, \dots, o^{m,d}, \dots, o^{IP,q'}, \dots, o^{m,d'}, \dots o_X^{IP} >$$

The operations in the privacy protection mechanism may require new type of messages in the message set of the protocol in addition to the extension on the sequence of interaction protocol. Through accommodating privacy protection mechanism at the interaction protocol level, the interaction is limited to SO that privacy can be protected with an acceptable PPL in their interaction. The sequence of the operations in interaction protocol is not changed in the privacy based interaction protocol but the operations of the privacy protection mechanisms are applied. This can prevent or neutralize execution of non-authorized operations and transforming the sensitive implicit information to explicit. Each of the applied mechanisms has a PPL value. Several mechanisms can be integrated with an interaction protocol to form a privacy based interaction protocol(PB_IP). By putting an assumption on independency of the protection mechanisms, the PPL of the protocol becomes the multiplication of PPL of all applied mechanisms.

$$PPL(PB\_IP) = \prod_{\forall \mu_i \mid \in (\mu_i, PB\_IP), \in (\mu_i, M)} PPL(e_i, M(PB\_IP), \mu_i)$$

7. Privacy Aware Smart Object

The privacy protection management framework enables SO to identify the sensitive information by capturing the information and their exposure boundary. As such it will be able to identify the sensitive information and extend the interaction protocol with adequate privacy protection mechanisms without impacting the soundness of the protocol and the supporting architecture. This extends the interaction protocol to privacy based interaction protocol through which the SO applies for interaction.

The computation entity modelled as CIR-agent has the following elements:

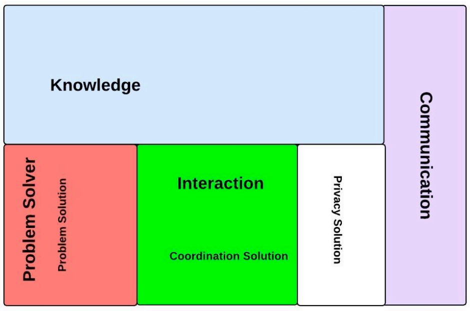


Figure 2. Privacy solution in relation with interaction in the computation entity in CDS environment

$$\text{Computation Entity} \equiv < K_i, PS_i, In_i, Com_i >$$

In information management form of computation, entities are modeled as information and operation.

$$\text{Information Management Entity } e_i \equiv < I_i, O_i >$$

This allows modeling the knowledge as set of information and operations as the following:

$$K_i \equiv < I_i^k, O_i^k >, \subseteq (I_i, I_i^k), \subseteq (O_i, O_i^k) \quad 1.$$

Also, problem solving can be modeled as operation in information management.

$$PS_i \equiv O_i^{ps}, \subset (O_i^{ps}, O_i) \quad 2.$$

Within information management context, the interaction can be modeled as information and operations

$$In_i \equiv < I_i^{In}, O_i^{In} >, \subset (I_i^{In}, I_i), \subset (O_i^{In}, O_i) \quad 3.$$

And the communication layer is modeled as information.

$$Com_i \equiv I_i^{com}, \subset (I_i^{com}, I_i) \quad 4.$$

As privacy is a characteristics of communication based interactions, the proposed framework resides between communication and interaction in CIR-agent architecture (Figure 2).

As described in the privacy protection management framework, interaction protocols can be modeled as sets of messages and sequences thereof:

$$IP \equiv < M, S_M > M \equiv \{m_1, \dots, m_m\}, 1 < m < Z$$

Each message in the interaction protocol conveys content; this content involves sending and receiving entity and operations that transfer the message.

$$m_{ij} \equiv < e_i, e_j, C_m, O_{i,m} >$$
$$, e_i : \text{Receiver}, e_j : \text{Sender}, C_m : \text{content}, \in (C_m, I_i), \in (O_{i,m}, O_i)$$
5.

Sequences are constructed by patterns of exchanging messages.

Assuming, M^k: All sequences in M with k length

Then
$M^* \equiv \bigcup_{k=1}^{X} M^k$, All possible sequqnces given the set M

Therefor, $S_M \subset M^*\ S_M = [s_1, \dots, s_q], 1 < q < Q$ 6.

Each sequence carries multiple messages

$$s_q = [m_{a+1}, \dots, m_{a+X}], 0 < a < V, 1 < X < Z \quad 7.$$

which can include several sub-sequences:

$$ss_{q,t} = [m_{a+l}, \dots, m_{a+p}], 1 < l, p < X, 1 < a < V, 1 < t < T, ss_{q,t}: \text{Subsequent of a sequence}$$
8.

Let s_q^* be the set of all subsequences of a sequence. Then:

$$s_q^* \equiv \bigcup_{1 \le t \le T} ss_{q,t} \, 9.$$

As messages are bound to operations that deliver them, $ss_{q,t}^o$ represents all of the operations of a subsequence:

$$ss_{q,t}^o \equiv \bigcup_{n=l}^{p} o \mid o \equiv O_{i,a+n} \wedge \in (m_{a+n}, ss_{q,t}) 10.$$

$$ss^u_{q,l} \equiv [o_{l,u,1,l}, \dots, o_{l,u,l,p}], 1 \le l, p \le X, 1 \le u \le V \quad 11.$$

Therefore, the execution of a the operations of a subsequence on the set of messages of an interaction protocol is denoted as

$$ss^u_{q,l}(M) \equiv o_{l,u,1}(C_{u,1}, o_{l,u,(l+1)}(\dots, o_{l,u,p}(C_{u,p}))) \quad 12.$$

To capture privacy at the computation level and provide protection mechanism, it is required to incorporate privacy in interactions. Interactions are steered by interaction protocols that can be modeled as messages and sequences of messages. Privacy Protection Management is responsible in identifying privacy concerns in interaction protocols and providing privacy based interaction protocol that encompasses the protection operations to protect privacy as depicted in Figure 3.

Privacy in the context of information management is the state of exposure boundary of information that includes entities for which sharing information can happen. Knowledge in the computation entity includes all information, intentions, believes as well as the exposure boundary of information

$$\subseteq (I_r, I^k_i), \forall k_r \in (E_{l,r}, I^k_i)$$

Information is shared through messages of interaction protocol. By capturing the receiver entities of the messages in the interaction protocol, the participating entities in the interaction will be identified. Based on equation 5:

Then, participating entities are through which it allows identifying the exposure boundaries:

$$R^e \equiv \bigcup_{m=1,s=1}^{c} e_m, e_s \mid \models (< e_s, e_m, C_m, O_{s,m} >, M),$$

13.

By applying the framework principles and given the exposure boundaries, the sensitive information can be captured as the following:

$$I^s_i \equiv \bigcup_{k=1,j=1}^{k \le N, j \le V} (I_{i,k}, e_j) \mid \models (e_j, (R^e - E_{i,k})),$$

14.

As depicted in Figure 3, the layer of "Sensitive Information" is adjacent to exposure boundary and interaction. This allows this layer to capture the necessary elements from the exposure boundary and interaction protocol to identify sensitive information.

Interaction protocol follows a sequence of messages among entities. These messages have content that carries required information to follow the protocol. In this context, messages are tied to operations that deliver the content from one entity to another. This positions messages in conjunction with operations equivalent to sharing.

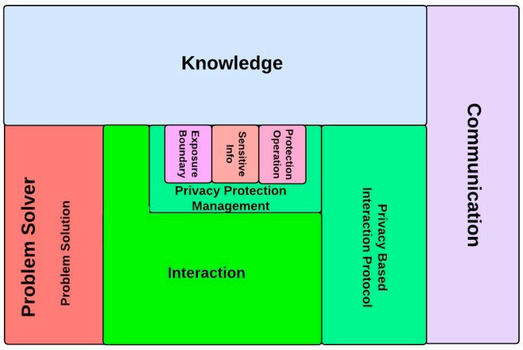


Figure 3. The logical architecture of privacy protection management in privacy aware SO

Considering equation 5:

$O_{s,m}$ delivers the messages transferred to the communication layer. Therefore: $O_{s,m} \equiv = (I^k_m, U(C_m, I^k_m))$

Based on equation 5 in the privacy protection management framework, Sharing C_m becomes the operation that results in addition of C_m to the information set.

The content of messages convey information that might disclose sensitive information in conjunction with other messages of the sequence. This results in disclosing sensitive information when the sequences of messages are exchanged. The sensitive information is computed by capturing the exposure boundaries. Therefore, evaluating sub-sequences of the interaction protocol to identify disclosing sensitive information is essential.

$$H^e \equiv \bigcup_{q=1,j=1,l=1,s=1}^{q \le Q, j \le V, l \le T, k \le N} (ss_{q,l}, I_{i,s}) \mid (= (ss^u_{q,l}(M), I_{i,s}) \wedge I^s(I_{i,k}, e_j))$$

15.

Also, non-sensitive information can be used as auxiliary information to transform implicit sensitive information to explicit. Typically, the preventive mechanisms cannot be applied for auxiliary information as they are shared within the exposure boundary. To deal with this, entities comply with agreements and applying punishing mechanisms. The concern regarding the auxiliary information can be identified through exploring the receivers and the information shared with them in a sequence of messages in the interaction protocol.

$$A^e_i \equiv \bigcup_{q=1,j=1,l=1,k=1}^{q \le Q, j \le V, l \le T, k \le N} ([o], I_{i,s}) \mid \models (o, ss^u_{q,l}) \wedge \pi \equiv S(I_{i,k}, e_j)$$

16.

Hence, the concern points in the interaction protocol can be identified as follows: $D^e_i \equiv U(H^e_i, A^e_i), D^e_i: \text{Concern points}$ 17.

Protection operations are part of the knowledge of the entity. Entities can utilize various protection operations that are registered within the knowledge of the entity. Protection mechanisms such as differential privacy anonymization [31], private bid-communication [30] and contractual operation execution [32] are examples of protection operations that can dynamically be registered in an entity and be applied on the interaction protocol. Each protection operation comes with the associated PPL that will be used as a measure to evaluate the privacy state of the privacy-based interaction protocol.

Protection Operation Registration:

$$Reg(e_i, \mu, PPL) \equiv = \left(U^k, \bigcup (O^k_i, \mu)\right) \wedge = \left(I^k, \bigcup (I^k, PPL(\mu))\right)$$

A protection operation in a computation entity when the $Requested\ PPL = \lambda$ is denoted as:

Protection Operation:

$$\mu_{i,s} \equiv \mu \mid \models (\mu, O^k_i) \wedge \exists j, \models ((i_{i,k}, e_j), I^s) \wedge \exists$$

$$\in (S, I_i) \wedge \models (I_{i,k}, S) \wedge PP(\mu|S) \wedge PPL(\mu) > \lambda$$

Depending on the sequence of messages in the interaction protocol and the identified privacy concern, an adequate protection operation is required to be applied. Based on the above definition, Protection Operation layer performs analysis on the given sequences and the expected PPL value to retrieve the adequate protection operation among available protection operations.

The privacy protection management framework introduces three forms of expansions in interaction protocol: prefixing, appending and generic. In the generic forms of expansion, for each of subsequences tagged as concern point, the privacy-based sequence will be substituted with the original one. The concerns marked as auxiliary will be extended with punishing protection operations as well as the structure to include the adequate agreements.

Depending on the content that is shared in a subsequence, it might be tagged as concern point multiple times. Let $\lambda_{i,l}$ be the sensitive information that $ss_{q,l}$ is tagged for. Based on equation 11 and 15:

$$\lambda_{i,l} \equiv \bigcup_{k=1}^{i\geq N} I_{l,k} \mid \in ((ss_{q,l}, I_{l,i}), H_i^*)\lambda_{q,..} \equiv \{I_{l,k}, \dots, I_{l,i}\}$$

Then we can retrieve the protection record of the information in $\lambda_{i,l}$

$$\mu(\lambda_{i,l}) \equiv \bigcup_{k=1}^{i\geq N} \mu_{l,k} \mid \in (I_{l,k}, \lambda_{q,l})$$

and let $\lambda'_{q,l}$ be the information that might be used as auxiliary information in a sequence:

$$\lambda'_{q,l} \equiv \bigcup_{k=1}^{k\leq h} I_{l,i} \mid (ss_{q,l}, I_{l,k}) \in A_i^*\ \lambda'_{q,..} \equiv \{I_{l,k}, \dots, I_{l,m}\}$$

Similarly the protection record of the information in $\lambda'_{q,l}$ is

$$\mu(\lambda'_{q,l}) \equiv \bigcup_{k=1}^{k\leq h} \mu_{l,i} \mid I_{l,k} \in \lambda'_{q,l}$$

Also, $ss''_{q,l} \equiv [u_{l a l b}, \dots, u_{l a l p}], 1 < l, p < X, 1 < a < V$ 18.

Then

$$PB\_Seq(ss_{q,l}) \equiv Pun(Prev(ss''_{q,l}, \mu(\lambda_{q,l})), \mu(\lambda'_{q,..}))$$ 19.

$$Prev(ss''_{i,l}, \mu(\lambda_{i,l})) \equiv Prefixing(ss''_{i,l}, \mu(\lambda_{i,l}))$$ 20.

$$Pun(ss''_{q,l}, \mu(\lambda'_{q,..})) \equiv Prefixing([<Agreement.Reject>, <Agreement.Confirm>], Appending(ss''_{i,l}, \mu(\lambda'_{q,..})))$$ 21.

The privacy based sequence for the subsequences that do not belong to concern points will stay as the original subsequence. This is due to $\mu(\lambda_{i,l}) \equiv \emptyset$ and $\mu(\lambda'_{q,l}) \equiv \emptyset$.

The sequences of the privacy-based interaction protocol are the set of all sequences or their privacy based sequences substitutions if they are among the concern points.

$$PB\_S_M \equiv \bigcup_{i=1,l=1}^{i\leq|I|, l\leq T} PB\_Seq(ss_{i,l})$$

22.

The messages that are exchanged in these sequences will form the set of messages that the privacy-based interaction protocol utilizes.

$$PB_M \equiv \bigcup_{q=1,l=1,s=1,r=1}^{q\leq|I|, l\leq T, s\leq 1, r\leq 1} < e_q, e_r, C_m, U_{x,m} > \mid \in (O_{a,m}, ss''_{q,l}), \in (C_m, I_l), \in (e_r,$$

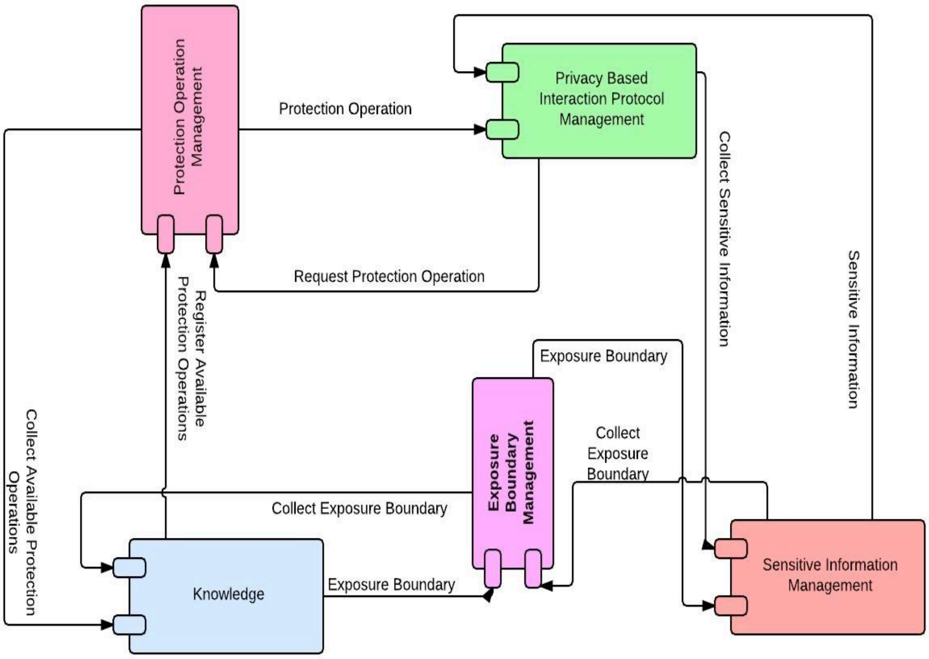

Protection Operation Management
Protection Operation
Privacy Based Interaction Protocol Management
Collect Sensitive Information
Sensitive Information
Request Protection Operation
Register Available Protection Operations
Collect Available Protection Operations
Exposure Boundary
Exposure Boundary Management
Collect Exposure Boundary
Collect Exposure Boundary
Knowledge
Exposure Boundary
Sensitive Information Management

Figure 4. The Competent architecture of Privacy Protection Management in Computation entity

23.

This completes the necessary elements to present the privacy-based interaction protocol. $PB\_IP = < PB_{sq}, PB\_S_{sq} >$

8. Implementation Challenges

The sequences of the privacy-based interaction protocol include the set of substitution of all sequences that belong to concern points or and their message types.as indicated in equation 22 and 23. Accordingly, the privacy protection can be incorporated in the privacy aware SO. The component diagram of the privacy protection management is presented in Figure 4.

JIAC (Java Intelligent Agent Component) is a framework for developing distributed heterogeneous, complex systems. This platform supports the developments of Multi-Agent Systems (MAS) through features such as [24]: Spring-Based Component System, ActiveMQ-based messaging, JMX-based management and Transparent distribution

Applying the privacy protection management framework at the computation level, requires expanding on the computation entity. JIAC platform enables developing distributed decentralized setting in which the communication and agent life cycle management is steered by the platform. JIAC applications typically inherit decentralized distributed context, which consist of multiple Agent Nodes. The AgentNode is a computation-service platform that is architected as distributed layer providing services to agents. Actions are part of the trait of agent beans in JIAC that allows the asynchronous execution of behaviors in agents. All the operations including the protection operations and interaction operations are implemented as an action in the JIAC platform. Actions can be added dynamically to the memory of the agent. It can scale up to the agent node as well as direct the agent to be accessible by search inquiries. In this work, we have introduced the actions at node level. Actions are searched by template specification which specifies that characteristics of an action to be called. When the protection operations are registered, the template of their action is added to the agent and it will be called when the action is searched through the agent memory. Actions can perform send operations as well as performing processing operations. The flexibility of the dynamic action allowed us to implement the operations of the sequences of the interaction protocol as an action within an agent. Before the agent gets to the ready state, the action list is updated so that the agent accesses the necessary actions.

Figure 5 shows part of the execution of the bean that dynamically adds the template of the action to the agent.

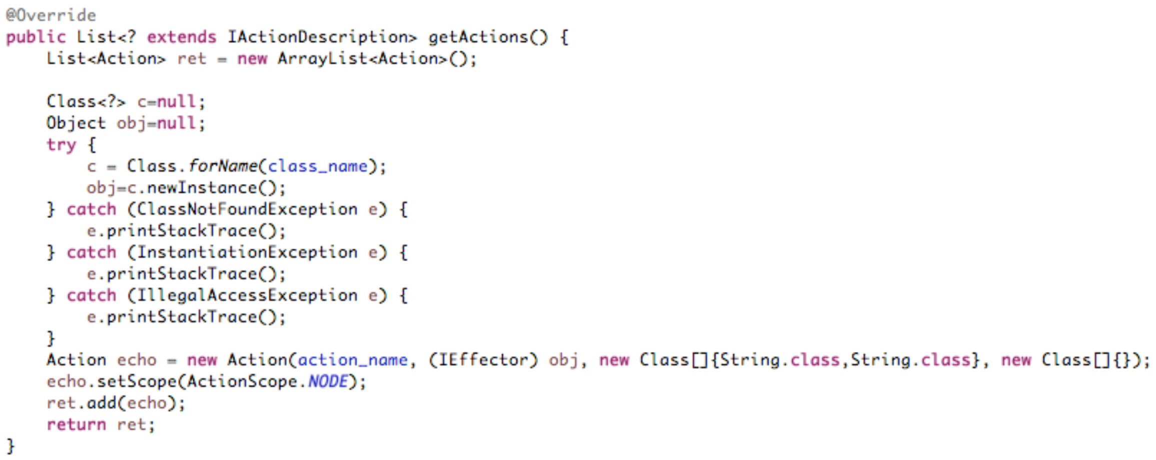
The following is the details of implementation of privacy aware computation entity within JIAC agent platform. Some of the proposed components are employed to resolve the requirements and restriction of implementation platform.

In JIAC application, interaction sequences can be modelled as set of actions that performed by entities. Each of the messages and protection operations is captured as actions.

The Privacy Protection Management expands the interaction protocol with adequate protection operations and provides privacy based interaction protocol. Privacy Based Interaction Protocol manages all interactions of the computation entity with others through which the adequate privacy protection operations are applied. The messages and sequences of messages that are sent for communication are managed by the privacy aware interaction protocol. The functionalities of this layer can be categorized as follows: A) Expanding the message indexes with the new and modified message types. B) Managing sequences of the protocol upon receiving new messages when entities interact.A is packaged as the functionalities of "Action_Management" component in the component architecture diagram. B is the functionality of the "Sequence_Manegemt" component in the component diagram. The component architecture is shown in Figure 6.

9 Conclusion

Internet of things encompasses a vast number of applications that are currently part of people's lives. They include "things" that can be modelled as smart objects (SO) and can seamlessly communicate with each other in an internet based interconnected platform. "things" in IoT actively participate in the environment to deliver the services of applications. In this work, a CDS model of IoT is proposed and smart objects are modelled as CIR-Agents. Due to the increase of involvements of people or their devices in IoT applications, privacy concerns have become a major challenge. In this setting SO possess sensitive information and they are reluctant to share them. Sensitivity of information has been defined within an exposure boundary containing SOs that the information can be shared within. Preventing or neutralizing non-authorized operations from execution on information is the main concern of privacy protection. the proposed model considers PPL as a measure to address the uncertainty level in privacy protection mechanisms. The privacy protection management framework defines privacy-based interaction protocol and protection operations for CDS-based IoT applications. Incorporating the proposed privacy model at the architecture, enables the SOs to become privacy-aware and thus the computation solutions inherit the privacy protection at the interaction level.



```
@Override
public List<? extends IActionDescription> getActions() {
    List<Action> ret = new ArrayList<Action>();

    Class<?> c=null;
    Object obj=null;
    try {
        c = Class.forName(class_name);
        obj=c.newInstance();
    } catch (ClassNotFoundException e) {
        e.printStackTrace();
    } catch (InstantiationException e) {
        e.printStackTrace();
    } catch (IllegalAccessException e) {
        e.printStackTrace();
    }
    Action echo = new Action(action_name, (IEffector) obj, new Class[]{String.class,String.class}, new Class[]{});
    echo.setScope(ActionScope.NODE);
    ret.add(echo);
    return ret;
}
```

Figure 5. Adding Dynamic Action to the agent at Node level

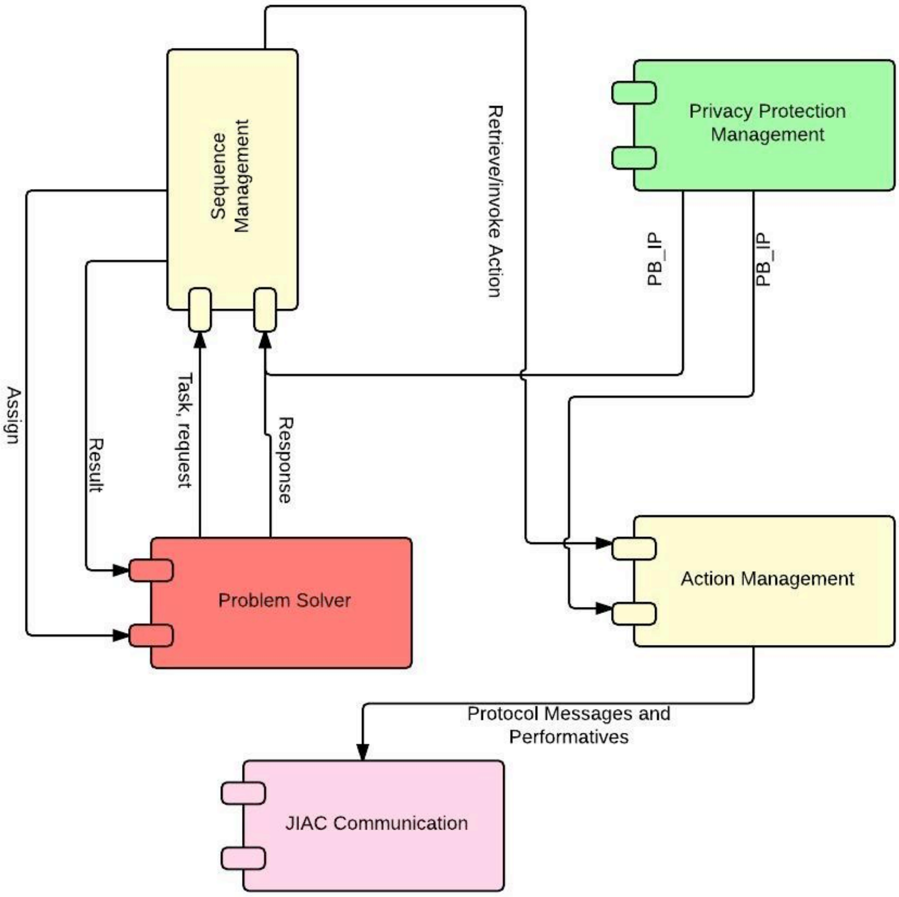


Figure 6. Component diagram of the implemented JIAC agent

References

[1] L. Atzori, A. Iera and G. Morabito. From smart objects to social objects: The next evolutionary step of the internet of things. IEEE Communications Magazine 52(1), pp. 97-105. 2014. Available: http://dblp.uni-trier.de/db/journals/cm/cm52.html#AtzoriIM14. http://dx.doi.org/10.1109/MCOM.2014.6710070

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

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

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

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

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

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

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

[9] Bo Lang , Ian Foster , Frank Siebenlist , Rachana Ananthakrishnan , Tim Freeman, "A Multipolicy Authorization Framework for Grid Security," Proceedings of the Fifth IEEE Symposium on Network Computing and Application, 2006. http://dx.doi.org/10.1109/NCA.2006.4

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

[11] A. Machanavajjhala, D. Kifer, J. Gehrke and M. Venkitasubramaniam. L-diversity: Privacy beyond k-

anonymity. ACM Trans.Knowl.Discov.Data 1(1), 2007. Available: http://doi.acm.org/10.1145/1217299.1217302. DOI: 10.1145/1217299.1217302. http://dx.doi.org/10.1145/1217299.1217302

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

[13] (March 19, 2014). Facebook's facial recognition software is now as accurate as the human brain, but what now?. Available: http://www.extremetech.com/extreme/178777-facebooks-facial-recognition-software-is-now-as-accurate-as-the-human-brain-but-what-now.

[14] (March 17, 2014). Facebook Creates Software That Matches Faces Almost as Well as You Do. Available: http://www.technologyreview.com/news/525586/facebook-creates-software-that-matches-faces-almost-as-well-as-you-do/.

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

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

[17] I. Kayes and A. Iamnitchi. Aegis: A semantic implementation of privacy as contextual integrity in social ecosystems. Presented at Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference On. 2013, . DOI: 10.1109/PST.2013.6596041. http://dx.doi.org/10.1109/PST.2013.6596041

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

[19] B. K. Sy, A. Ramirez and A. P. K. Krishnan. Secure information processing with privacy assurance - standard based design and development for biometric applications. Presented at Privacy Security and Trust (PST), 2010 Eighth Annual International Conference. 2010, . DOI: 10.1109/PST.2010.5593255. http://dx.doi.org/10.1109/PST.2010.5593255

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

[21] R. Dong, A. A. C\'ardenas, L. J. Ratliff, H. Ohlsson and S. S. Sastry. Quantifying the utility-privacy tradeoff in the smart grid. CoRR abs/1406.25682014. Available: http://arxiv.org/abs/1406.2568.

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

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

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

[25] F. Mattern and C. Floerkemeier. From the Internet of Computers to the Internet of Things.2010.

[26] T. C. McCourt, S. Leopold, F. G. Louthan IV, H. Mosesmann, J. S. Smigie, T. Tillman, D. Toomey, G.Kyriakopoulos, E. Lemus, B. Peterson and A. Sklar. The Internet of Things A Study in Hype Reality Disruption-and Growth. Raymond James & Associates, Inc, 2014.

[27] Z. Pang. Technologies and Architectures of the Internet-of-Things (IoT) for Health and Well-being. Royal Intitute of Technology (KTH) Sweden. 2013.

[28] R. Chitkara, W. Ballhaus, O. Acker, B. Song, A. Sundaram and M. Popova. The Internet of Things: The next growth engine for the semiconductor industry. Published by PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft, 2015.

[29] V. Nguyen and A. Gendreau. A Vision of a Future IoT Architecture Supporting Messaging, Storage, and Computation. International Journal of Future Computer and Communication, Vol. 3, No. 6, December 2014.

[30] I. Damgard, M. Geisler and M. Kroigard. Homomorphic encryption and secure comparison. Int.J.Appl.Cryptol. 1(1), pp. 22-31. 2008. http://dx.doi.org/10.1504/IJACT.2008.017048

[31] C. Dwork, F. McSherry, K. Nissim and A. Smith. Calibrating noise to sensitivity in private data analysis. Presented at Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006. 2006. http://dx.doi.org/10.1007/11681878_14

[32] L. Crepin, Y. Demazeau, O. Boissier and F. Jacquenet. Sensitive data transaction in hippocratic multi-agent systems. Engineering Societies in the Agents World IX, A. Artikis, er, G. Picard and L. Vercouter, Eds. 2009.