Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 52 (2015) 606 – 613

Procedia Computer Science

The 6th International Conference on Ambient Systems, Networks and Technologies (ANT 2015)

Privacy in Internet of Things: A Model and Protection Framework

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

A new form of computation is being evolved to include massive number of diverse set of conventional computing systems, sensors, devices, equipments, software and information services and apps. This new form of computing environment is known as the "Internet-of-Things" (IoT). The adoption of IoT is fast and the "things" are becoming integral part of people day-to-day life as well as essential elements in the businesses everyday activities and processes. Open characteristics of IoT environments raises privacy concern as "things" are autonomous with some degree of authority to sharing their capabilities and knowledge to fulfil their individual or collective tasks. As such privacy becomes central and an inherit computational aspect of the "things". The work presented here is based on modelling IoT as Cooperative Distributed Systems (CDS). It proposes a novel approach of analysing and modelling privacy concepts and concerns. Privacy protection is captured as a form of "*sensitive information*" management at the interaction level. A privacy protection management framework for CDS at the interaction level is proposed. The application of the framework has been demonstrated by extending Contract Net Protocol (CNP) to support privacy protection for CDS.

Peer-review under responsibility of the Conference Program Chairs

Keywords: Privacy; IoT; Cooperative Distributed Systems (CDS).

* Corresponding author.
E-mail address: asamani5@uwo.ca, hghenniw@uwo.ca, amasaud@uaeu.ac.ae

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2015.05.046

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. They are able to communicate with each other via the Internet. The future growth of IoT based applications is foreseen to be tremendously high. Incorporation of social networks and ubiquitous computing technologies in IoT enables individuals and groups of people to engage seamlessly with the environment [1]. The comfort that is experienced through the innovative technologies in IoT was with the expenses of privacy [2], [3]. For instance, processing the sensor information of houses that their hallways and doors are equipped with light and magnet sensors can infer the layout of the building which might be exploited in malicious objectives. In another example, 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 such as anonymization [4], utility tradeoffs [5], 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 an integral part of the computation platform. This requires treating privacy as a mathematical object and incorporating it as a quality factor for the solutions that are computed. As a result, resolving privacy in IoT entails modelling IoT as a computational platform. This paper proposes modelling IoT as Cooperative Distributed Systems (CDS) as the computation platform in which entities are autonomous and self-interested. Entities are expected to have some degree of authority in sharing their information and capabilities with others. The interaction is carried through exchange of messages [8]. 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.

The current approaches for privacy protection in distributed heterogeneous environments such as IoT can be classified into two main categories: rule-based approaches and architectural-based approaches. The privacy solution models that are derived from rule based models typically designed for closed environments. These approaches are mainly concentrate on applying rules over shared information. Because of the open environment assumption in IoT the rule-based approaches [9] are not adequate [10]. Among architectural based privacy solutions are anonymization techniques [4], [11], privacy utility trade off mechanisms, [5], [12], social tradeoffs and proxy based privacy protection [6]. However, in this context, the anonymization techniques are limited to a particular setting including participants, information collector and an adversary that makes attempt to collect individualized information from the information collector. There is an assumption in this setting that the information collector is a trusted party. These mechanisms are tailored towards protecting the sensitive information such as participation of "things" in information collecting process. They do not address the disclosure of aggregated information that is attributed to "things" [4]. The utility trade off mechanisms are based on evaluating the information gain of the exchanged information [5].

This paper proposes architecture based privacy protection framework. The rest of the paper is structured as follows. Section 2 explicates some of characteristics of IoT environment and models it as CDS. Section 3 presents a model for privacy in CDS model. Section 4 elaborates on a framework for managing privacy protection at interaction level for CDS-based IoT. Finally, the work is concluded in section 5.

2. 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 Cooperative Distributed System (CDS) in which entities are Smart Objects (SO) that are capable of performing capabilities with ability to coordinate their activities with others to achieve individual or collective goals. SO can be autonomous and self-interested with incomplete knowledge. In this context, SO represent "things" that are capable of sharing information and making decision based on self-interested objectives.

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].

3. Privacy: 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: $\mathrm{W} = \{\mathrm{e}_1, \dots, \mathrm{e}_\mathrm{N}\}$,

In the context of information management, entities can be modelled as operations and information. $\mathrm{e_i} =< \mathrm{O_i}, \mathrm{I_i} >$, $1 \le i \le N$ $\mathrm{I_i} \equiv \{\mathrm{I_{i,1}}, \dots, \mathrm{I_{i,k}}, \dots, \mathrm{I_{i,M}}\}, 1 \le \mathrm{i} \le \mathrm{N}, 1 \le \mathrm{k} \le \mathrm{M}$, $\mathrm{O_i} \equiv \{\mathrm{o_{i,1}}, \dots, \mathrm{o_{i,w}}, \dots, \mathrm{o_{i,W}}\}, 1 \le \mathrm{i} \le \mathrm{N}, 1 \le \mathrm{w} \le \mathrm{W}$

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 $\mathrm{E_{i,k}}$ be the exposure boundary that is designated by the smart object e_i for $I_{i,k}$: $\mathrm{E_{i,k}} \equiv \{\mathrm{e_{t+1}}, \dots, \mathrm{e_{t+r}}\}, 1 \le \mathrm{r}, \mathrm{t} \le \mathrm{N}, \subset (\mathrm{E_{i,k}}, \mathrm{W})$

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 $\mathrm{E_{i,k}}$.

Information can also be exhibited as implicit. "*Implicit information"* can be transformed to explicit by the execution of some operation $o(I^{x1}, I^{aux})$. Manipulation of explicit information $\mathrm{I^{x1}}$ by processing operations can transform the implicit information into explicit form I^{x2} through execution of the operation which is denoted as: $\bar{o}(I^{x1}, I^{aux}, I^{x2})$. 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 smart objects 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 $O_j^{i,k}$ that is a set of operations belonging to O_j where e_i has agreed on applying them on $I_{i,k}$. 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 $\hat{o}_{j,t}^{i,k}$ is considered a form of "*privacy violation"*.

$Let\ \hat{O}_j^{i,k} \equiv \{\hat{o}_{j,1}^{i,k}, \dots, \hat{o}_{j,t}^{i,k}, \dots, \hat{o}_{j,T}^{i,k}\}, 1 \leq t \leq T$. Similarly,

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

refers to all possible non-authorized operations and for a set of information

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

Let $\downarrow \hat{O}_{j,w}^{i,k}$ be not allowing execution of $\hat{o}_{j,w}^{i,k}$. And let $\theta_{i,j}^{i,k} \equiv \forall w \mid \downarrow \hat{O}_{j,w}^{i,k}$ be the agreement between e_i and e_j. Accordingly the privacy violation becomes:

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

Now, let $\bar{\delta}(\widetilde{I^{x1}, I^{aux}})$ be the inability of SO to execute the non authorized operation either by preventing or neutralizing the operation. "*Privacy protection*" then can be defined as the enforcement mechanisms to prevent or to neutralize the application of non-authorized operations on shared information.

$$PP(e_j, (PS(I_i)), \hat{O}_j) \equiv \forall t, w \mid (t, PS(I_i)) \wedge \widetilde{\bar{\bar{\delta}}_{j,w}^{t}(t)}$$

Where $PS(S) \equiv S' \mid \forall p, \in (p, S') \wedge \subset (p, S) \wedge (\nexists p' \mid \subset (p', S) \wedge \not\subset (p', S'))$

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].

4. Privacy Protection Management 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: $\bar{\mu} \equiv PP\left(e_j, S, \hat{O}_j^i(S)\right)$

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: $PPL(e_j, I_i, \mu_t) = P(\bar{\mu} \mid I_i)$. As an example of protection mechanism is a $\epsilon-$differential private function is $(1 - 2\epsilon)$ [17]. The expected value of having differential privacy in n number of times experimenting it becomes

$E(z) = n(1 - 2\epsilon)$. This corresponds to PPL with a value given by $1 - 2\epsilon$.

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 modeled 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.

4.1. 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 $< \delta, e_i, e_j, IP >$ where δ is the kind of interdependency; e_i and e_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 $IP =< o^{IP,1}, \dots, o^{IP,q}, \dots, o^{m,Q} >$.

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

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:

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

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.

$$PPL(PB\_IP) \;=\; \coprod_{\forall\, \mu,j \;|\; \in(\mu,PB\_IP),\in(e_j,W)} PPL(e_j, \mathrm{M(PB\_IP)}, \mu))$$

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.

Contract Net Protocol (CNP) is an interaction protocol that was initially proposed for distributed problem solving a special class of CDS. This protocol can be employed to solve the capability-based interdependency. The protocol identifies several roles for the participant entities, including manager that announces a task and potential contractors that might be capable of executing the task will compete. The potential contractors that can perform the task best is awarded with the task becomes the contractor and delivers the result after executing it [19]. CNP can be applied for SO in IoT and adopt a brokering architecture where the manager is represented by the role of brokers and the requesters delegate their tasks to the broker [manager]. A smart space project has been implemented as an IoT environment in CDS-ENG research laboratory. It includes sensors, equipments, services and data resources that are exposed to applications. Within this environment, there are smart objects constructing the "things" layer. Services in this environment utilize the existing resources in the space and deliver solutions to applications. The brokering layer provides functionalities to integrate with resources of the environment including data, services, clouds and events.

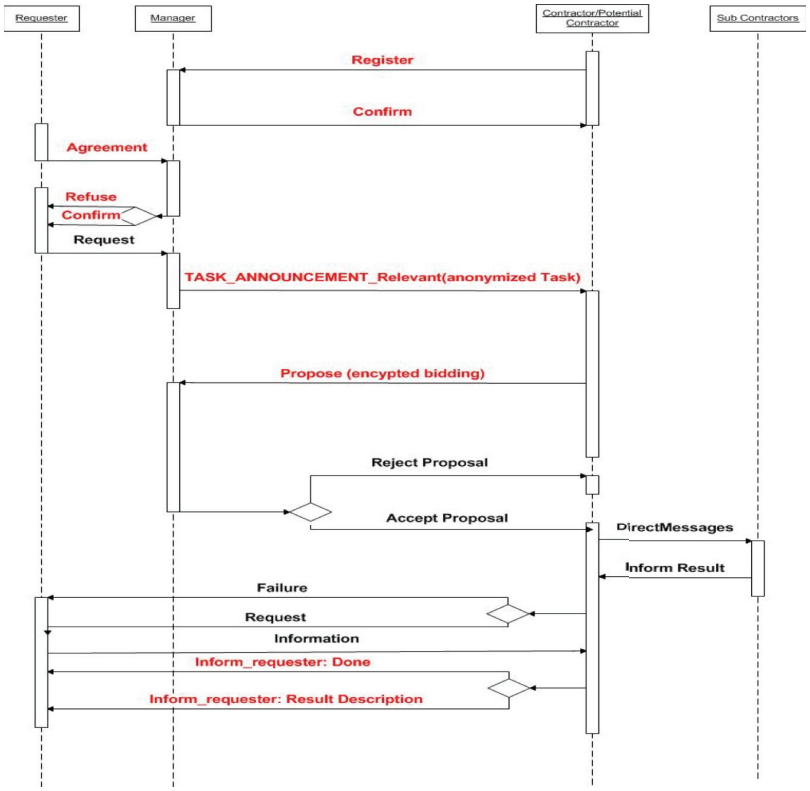

Fig 1. Privacy based CNP

To resolve the capability interdependency in such setting, smart objects adopted CNP as the interaction protocol where the brokering layer acts as the manager entity. The operation-based presentation of CNP can be modeled as:

$CNP = \{< Request(TaskAnnouncement), Task\_Announcement(), Propose(Bid), Accept\_Prop, Inform,$

$Response >, < Task\_Announcement(task), Propose(Bid), Reject\_Prop >, < Task\_Announcement(task), Reject >\}$

Smart objects share information using the message types and sequences of messages in CNP. However, privacy concerns in sharing information in CNP is not considered and providing privacy protection at this protocol is lacking. In this protocol, $I_{r,t} = \{association\ of\ tasks\ to\ requester\}$ and exposure boundary $I_{r,t}$ is $E_{r,t} = \{manager\}$; $I_{c,b} = \{\text{biding information}\}$ and the exposure boundary $I_{c,b}$ is $E_{c,b} = \emptyset$; $I_{r,j} = \{\text{result information of execution}\}$and the exposure boundary of $I_{r,j}$ is $E_{r,j} = \{Contractor\}$

When SO follow CNP to identify another SO that is capable of performing their task, they start task announcement phase in CNP. The task announcement includes the identity of the requester and the task specification. Task announcement is shared with all SO with the purpose of finding potential contractors competing for the task. The exposure boundary of combination of task and identity of the requester only includes the manager. Hence, this information becomes sensitive. In the context of information management, CNP at this state is as the following: $CNP: [Request(TaskAnnouncement); TaskAnnouncement]$. As the result, the framework applies protection mechanism at the information level as it is adequate for task and identification broadcast to potential contractors. An example of such mechanism is anonymization techniques. Also to reduce the potential contractors the SO that have the capability related to the task, we have introduced the registration process at the beginning of the protocol. Because the information is shared with the manager and they may serve as auxiliary information at manager's side, applying preventive mechanism might not be possible. This suggests integrating punishing mechanisms. For the state of task announcement, privacy based CNP will be as the following: $CNP: [Request(TaskAnnouncement); Task\_Announcement\_Relevant(Annonymized\ Task)]$

In another part of CNP, the bidding information in conjunction with the identity of the potential contractors will be sent to participate in winner determination in the manager [broker] entity. The combination of the bidding value and the identity of the bidder is sensitive in relation with the manager [20]. This is due to the exposure boundary of this information which is $E_{c,b} = \emptyset$. However, CNP shares this information: $CNP: [Propose, Accept\_Proposal]$. One of the mechanisms to protect privacy in this context is applying preventive mechanisms at the information level using the mechanism proposed in [21] at which calculation happens on encrypted information and the broker is not aware of the bidding values. Utilizing this mechanism will extend the protocol with additional processes to encrypt the bidding information. $PB\_CNP: [BidEncryption, Propose, Accept\_Proposal]$

$E_{r,j}$ only includes the contractor which deduces that the result information is sensitive in relation with the manager. However, the traditional CNP shares this information with the manager. To protect this information, it is required to prevent the sharing operation (preventive mechanism at the operation level). This enforces the contractor to identify the owner of the task and directly send the information to them. Also it is possible to use cryptographic approaches to encrypt the result information with requester public key (preventive mechanism at the information level). In either of cases, the contractor has to perform a procedure to realize the owner of the request. $CNP: [Inform]$ and PB_CNP: [ONWER_REALIZATION, InformRequester]. Applying the proposed operations will expand the protocol in terms of messages and applying protection mechanisms as the following. The privacy based CNP is also depicted in Fig 1. PB_CNP = {< Agreement, Confirm, Request(TaskAnnouncement), Task_Announcement(anonymized task), Propose(Encrypted Bid), Accept_Prop, InformRequester >, < $Task\_Announcement$(anonymized task), Propose(Encrypted Bid), Reject_Prop >, < $Task\_Announcement$(anonymized task), Reject >, < Register, Confirm >}

To elaborate on the application of the privacy based CNP, let "Motion Detection" application be the smart object e_m that is using motion detection sensors in smart space but it requires capabilities of other smart objects to be equipped with light sensors, face detection, vibration detection and temperature measurements. Based on the structure of CNP, "Motion Detection" provides task announcement to the service broker to identify smart objects that are capable of executing the task. In the context of smart space W, e_m creates task announcement messages for light sensing ($I_{m,l}$) , face detection ($I_{m,f}$) , vibration detection ($I_{m,v}$) and temperature measurements ($I_{m,t}$). e_m is delivering safety and security services ($I_{m,s}$) to entities that are located in a museum ($I_{m,g}$). Operation o^{rec} is an operation that can predict next actions of entities based on their interests with some degree of uncertainty. Execution

of $\bar{\delta}^{rec}\left(\{I_{m,l}, I_{m,f}, I_{m,v}, I_{m,g}\}, I^{aux}\right) = I_{m,s}$. However, by applying the PB_CNP, the tasks are anonymized and the sensitive information is protected.

5. 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. However, because of the increase of involvements of people or their devices in these applications, privacy concerns have become a major challenge. In this work, a CDS model of IoT is proposed. 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. This work proposed PPL as a measure to address the uncertainty level in privacy protection mechanisms. In result, this work has proposed a privacy protection management framework that is associable in CDS-based IoT applications. It uses the interaction protocol and protection operations to generate a privacy based interaction protocol. The application of the privacy protection management framework on contract net protocol is presented in this work.

References

1. Atzori L, Iera A, Morabito G. From smart objects to social objects: The next evolutionary step of the internet of things. IEEE Communications Magazine 2014;52(1):97-105.
2. Adaptive security and privacy management for the internet of things (ASPI 2013). Proceedings of the 2013 ACM conference on pervasive and ubiquitous computing adjunct publicationNew York, NY, USA: ACM; 2013. .
3. Negotiation-based privacy preservation scheme in internet of things platform. Proceedings of the first international conference on security of internet of thingsNew York, NY, USA: ACM; 2012. .
4. Differential privacy: A survey of results. Proceedings of the 5th international conference on theory and applications of models of computationBerlin, Heidelberg: Springer-Verlag; 2008. .
5. A utility-theoretic approach to privacy and personalization. Proceedings of the 23rd national conference on artificial intelligence - volume 2AAAI Press; 2008. .
6. Such JM, Espinosa A, García-Fornes A. A survey of privacy in multi-agent systems. Knowl Eng Rev 2012.
7. Toubiana V, Nissenbaum H, Narayanan A, Barocas S, Boneh D. Adnostic: Privacy preserving targeted advertising □. 2010.
8. Ghenniwa HH. 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.
10. Paul M. Schwartz, Daniel J. Solove. The PII problem: Privacy and a new concept of personally identifiable information. 2011.
11. Machanavajjhala A, Kifer D, Gehrke J, Venkitasubramaniam M. L-diversity: Privacy beyond k-anonymity. ACM Trans.Knowl.Discov.Data 2007 mar;1(1).
12. On the tradeoff between privacy and utility in data publishing. KDD} '09: Proceedings of the 15th {ACM} {SIGKDD} international conference on knowledge discovery and data miningNew York, {NY {USA}: ACM}; 2009. 0036.
13. Facebook's facial recognition software is now as accurate as the human brain, but what now? [Internet].
14. Facebook Creates Software That Matches Faces Almost as Well as You Do [Internet].
15. Samani A, Ghenniwa HH. Privacy in IoT: A model and protection framework. London Ontario: ; August 2014. Report nr CDS-EnG-report-Privacy in IoT: A Model and Protection Framework-TR -0827 2014.
16. Sweeney L. K-anonymity: A model for protecting privacy. Int.J.Uncertain.Fuzziness Knowl.-Based Syst. 2002 oct;10(5):557-70.
17. Mechanism design via differential privacy. Proceedings of the 48th annual IEEE symposium on foundations of computer scienceWashington, DC, USA: IEEE Computer Society; 2007. .
18. Targeted advertising ... and privacy too. Proceedings of the 2001 conference on topics in cryptology: The cryptographer's track at RSALondon, UK, UK: Springer-Verlag; 2001. .
19. Smith RG. Computers, IEEE Transactions on Title={the Contract Net Protocol: High-Level Communication and Control in a Distributed Problem Solver 1980 dec.;C-29(12):1104.
20. Privacy preserving auctions and mechanism design. Proceedings of the 1st ACM conference on electronic commerceNew York, NY, USA: ACM; 1999.
21. Secure combinatorial auctions by dynamic programming with polynomial secret sharing. In proceedings of the sixth international financial cryptography conference Springer; 2002.