Sensitivity Level-Based Citizen Personal Information Model for Privacy Protection

Abdullah Alqahtani[1*], Haiyan Lu[1], Jie Lu[1]

[1] Decision System & e-Service Intelligence (DeSl) Lab, Center for Quantum Computation and Intelligent Systems (QCIS), Faculty of Engineering and Information Technology, University of Technology Sydney, Australia.

* Corresponding author. email: Abdullah.AlQahtani@student.uts.edu.au
Manuscript submitted February 10, 2014; accepted November 12, 2014.

Abstract: Citizens' privacy concerns have become a major barrier to their acceptance of e-government services, and the question of how to address these privacy issues effectively is increasingly important as government pushes service delivery online. Good protection of citizens' privacy will contribute significantly to the success of e-government services. Therefore, it is highly desirable to take into account privacy issues in e-government service integration to ensure the success of e-government services. On the one hand, there are many challenges in addressing the privacy issues in e-government service integration because users' personal information is often required for consuming e-government services and can potentially be accessed by different types of users (citizens and employees) at various government agencies. In addition, many aspects should be addressed in designing a privacy model. Several solutions have been recently proposed in the literature to deal with privacy concerns. However, there are few practical approaches for helping citizens to create their preferences for privacy protection. Ontology is considered one of the most powerful conceptual approaches to capture knowledge relevant to privacy aspects. Though ontologies for privacy have been suggested, they do not support citizens in setting up their privacy preferences based on various aspects of privacy policy, such as purpose, retention and consent. This paper proposes a new Sensitivity Level-Based Citizen Personal Information Model (SLBCPIM) that can facilitate citizens' role in controlling privacy preferences. This model organises the personal data item of a citizen into a number of sensitivity levels and links these levels with different privacy protection levels to satisfy the citizen's needs. It allows a citizen to set up his or her privacy preferences and supports computerisation of these preferences so that these preferences can be guaranteed. This model has been implemented as an ontology that is machine-readable and can be shared among e-government service systems. A simple Web-based application of this model is developed to validate the usefulness of this new model in supporting citizens in expressing their privacy preferences.

Key words: Ontology, e-government service, citizen privacy, sensitivity levels of personal information, privacy preference, privacy policy.

1. Introduction

The growth of the use of information and communications technologies has affected how citizens interact with governments, especially consuming online services in an e-government environment [1]. These technologies have also affected and will continue to affect how citizens' information is collected,

communicated, processed and stored [2]. Therefore, privacy problems in e-government grow in complexity as new, powerful and sophisticated technologies emerge. Furthermore, citizens' personal information collection by e-government has both benefits and risk implications. In terms of benefits, it is now possible for citizens to access more convenient services and save transaction time. In terms of risk, citizens could be required or forced to divulge personal information that could drive user concerns over possible malicious or accidental unauthorised divulgence of this information. Therefore, privacy and trust issues have received increasing attention from citizens, researchers and governments adopting e-government services.

In dealing with these privacy concerns, several solutions have been proposed, such as the P3P framework [3], IBM [4] and OASIS [5]. Unfortunately, although these solutions enforce access control mechanisms with privacy-related aspects, they fail to provide a chance for the citizen to specify his/her own privacy preferences for governing his/her own personal information—the government provider's policy is the only one offered, and it fails to guarantee the fate of a user's personal data.

In the light of the aforementioned issues, we propose a new and effective model based on ontology to increase citizens' control power over privacy-related aspects (such as retention, purpose, obligation, recipient and consent) and to provide facilities for citizens to express their privacy preferences. More specifically, this model can give citizens the chance to control the data that are collected and to whom it is disclosed and enable them to recognize that different situations may require different responses. The novelties of this work are threefold: 1) to introduce the concept of the Sensitivity Level-Based Citizen Personal Information Model (SLBCPIM) for dealing with citizens' personal information; 2) to propose a new ontology model-based SLBCPIM using sensitivity levels, a citizen personal information model and an ontology technique and 3) to apply this model in setting up citizens' privacy preferences. The two main advantages of using ontology are that the relationships_among different sensitivity-level concepts, citizen personal information model concepts and privacy policy concepts can be naturally represented using the ontology web language (OWL), and new relationships can be automatically inferred if necessary because ontology supports semantic reasoning.

The new SLBCPIM has been implemented by using an ontology modelling tool (e.g. Protégé) and evaluated by using the Pellet reasoner and SPRQL query, illustrated by examples. The illustration shows that the new model is powerful in allowing citizens to specify their privacy preferences effectively.

The rest of the paper is organised as follows: Section II presents related work. Section III describes the personal information of citizens regarding the use of e-government services and the sensitivity of individual personal information items. Section IV presents the model of citizen personal information, which is constructed based on sensitivity levels and privacy policy aspects. The construction process is briefly described, followed by a validation of the model using a set of competent questions. Section V illustrates how this model is employed in helping citizens to specify their privacy preferences when they use e-government services through a case study. Section VI presents the discussion and conclusions.

2. Literature Review

Privacy has become a buzzword as more and more e-government services are being offered over the Internet. There are a number of different definitions of privacy [6], such as information privacy and physical privacy. This indicates how difficult it is to address privacy issues effectively. In this work, we adopt the definition of privacy suggested by Alan Westin [7], which focuses on personal information privacy: 'the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'.

Based on the literature, a number of framework solutions for addressing privacy issues have been proposed. For example, the Platform for Privacy Preferences (P3P) Project [3] was proposed to provide a

way for a website to define its personal information privacy policy and to communicate it to the users who visit the site. Other approaches, such as IBM project [4] and OASIS [5], provide the automation of privacy policy enforcement. These frameworks focus on improving role-based access control based on privacy policy. However, these approaches are not suitable for giving citizens opportunities to control their personal information based on privacy policy because they aim at integrating access control and privacy policy.

An ontology is a formal representation of knowledge based on a set of concepts within a specific domain and relationships among the concepts [8]. It is a shared conceptualisation that provides shared vocabulary and taxonomy and can be used to model domains with the definition of objects, their relationships and their properties. An ontology can therefore be used to reason about and describe entities within a domain. In the literature, several ontology-based privacy frameworks have been proposed, where an ontology has been used as an effective way of capturing knowledge relevant to privacy. For example, Isaza *et al*. [9] present an ontology model for representing intrusion detection and prevention events. Qin and Atluri [10] use ontological mechanisms to implement access control at a conceptual level by associating concepts through their properties. However, these solutions refer only to security concepts and do not take other privacy aspects into consideration.

3. Proposed Sensitivity Level-Based Citizen Personal Information Model (SLBCPIM)

Each individual owns a set of personal information, such as his/her name, gender, date of birth (DOB), bank account details and contact details. The degrees of sensitivity of individual data items are very different; e.g., most people do not care about revealing their names, but almost everybody keeps his or her bank account details confidential. In using e-government services, it is inevitable to use some of the citizens' personal information, such as a personal identifier, DOB or bank account details. Making citizens feel safe about their personal information while they interact with an e-government service system is crucial for the success of e-government services. Although each e-government service provider has set up privacy policies for dealing with citizens' privacy, it seems that these policies are mainly for the sake of formality and do not distinguish sensitivity of individual information items, do not specify details about privacy policy aspects such as the purpose, retention, recipient, obligation and consent, and no guarantee is given. In this section, we propose a set of sensitivity levels for citizen personal information data item groups.

3.1. Citizen Personal Information Set

In this study, the 'citizen personal information set' refers to the data item collection that may be used to complete e-government services. Within the context of the e-government services offered in Saudi Arabia and Australia, the citizen personal information data items (CPIDI) are collected; for examples, Social Security Number, Passport Number.

These items can be classified into seven groups: identity information, birth information, including full name, marital status information, including gender, job information, contact information, financial information and education information. For example, Social Security Number and Passport Number are grouped in identity information group.

3.2. Privacy Policy

A privacy policy is a set of statements that are used as regulatory rules to protect the privacy of related entities. For the personal information of citizens, a privacy policy specifies the statements from the following five aspects: purpose, retention, recipient, obligation and consent. For each aspect, there are a number of options, such as no retention and deletion after use for the retention aspect. Table 1 lists the options for each privacy policy aspect.

3.3. Sensitivity Level Set for the Citizen Personal Information Data Item Group

Table 1. Privacy Policy Aspects with Options

Privacy Policy	Purpose	Marketing
		Development and Research
		Payment
		Profile
		Administration
		Citizen Request
	Obligation	No Obligation
		Delete after use
		Notification
	Consent	No Consent
		Disclosure Life Event Application to Parental Consent
		Disclosure Life Event Application to Research Consent
		Disclosure Life Event Application to Another Life Event Provider Consent
	Retention	No Retention
		Retention Time
		Indefinite Retention
	Recipient	Ours
		Unrelated
		Same Privacy Policy
		Different Privacy Policy

Table 2. Sensitivity Level Set for Identity information Group

CPISIG_ID	**Sensitivity Level**	**Privacy Policy**				
		Purpose	**Retention**	**Recipient**	**Obligation**	**Consent**
Social Security number (SSN)	Level 1	Citizen Request, Administrator, Profile	Retention Time	Ours	Delete after Use Notification	No Consent
	Level 2	Citizen Request, Profile	Retention Time	Ours	Delete after Use Notification	No Consent
	Level 3	Citizen Request, Administrator,	Retention Time	Ours	Delete after Use Notification	No Consent

The sensitivity level set defines a group of sensitivity levels for each group of citizen's personal information data item and each level of the sensitivity level consists of a privacy policy for each citizen personal information data item classified under one group. More specifically, each level of the sensitivity level set consists of a privacy policy for each citizen personal information data item classified under one group. For example, the sensitivity level set for the identity group will be described as level 1, level 2 and level 3 and each level consists of privacy aspects (purpose - retention - ..) as shown in Table 2. Also, the levels start from low level 'Level 1' to high level.

4. Designing Sensitivity Level-Based Citizen Personal Information Model as an Ontology

To support users in specifying their privacy preferences regarding personal information required by

e-government service and to allow citizens to set up their preferences for their personal information privacy, we have designed a new Sensitivity Level-Based Citizen Personal Information Model (SLBCPIM) to describe citizens' personal information clearly with the sensitivity level and privacy policy aspect taken into account using an ontology technique. This model provides an effective way to address privacy concerns that citizens may have within the context of e-government services.

This model is constructed as an ontology due to the fact that an ontology is a knowledge base and provides conceptualisation with a given domain, so it consists of a number of concepts (or classes), such as sensitivity level, citizen personal information and aspects of privacy and the relationships between these concepts with some constraints (or axioms). In developing this ontology model, we adopt the METHONTOLOGY approach, which is a structured method for building ontologies [11]. In the rest of this section, we present the processes of developing this ontology model.

4.1. Pre-design Phase

During this phase, the citizen personal information items were collected, such as Social Security Number (SSN), full name, and credit card number. These items are further_grouped with each group. The information items and groups are described in section III.

4.2. Design Phase

In this phase, a number of specific activities, such as specification, conceptualisation, formalisation and implementation needed to be carried out.

4.2.1. Specification

Based on the domain analysis, we determined the purpose and scope of this ontology model (SLBCPIM) as follows:

- To describe citizens' personal information within the context of e-government services;
- To describe the sensitivity levels of citizen personal information regarding the use of e-government services;
- To establish the relations between citizen personal information items/groups and options for privacy policy aspects through sensitivity levels; and
- To cater to citizens' needs when they express their privacy preferences within the context of using e-government services.

A number of competency questions [12], which this ontology model (SLBCPIM) must answer, were designed as follows for testing the final model against the specifications:

1) What are citizen personal information data items (CPIDI) in the context of using e-government services?
2) What are citizen personal information groups (CPIDIG)?
3) What are citizen personal information data items for each citizen personal information data items group?
4) What are the sensitivity levels for each CPIDIG that are used by citizens to determine their privacy preferences?
5) What are the options for each privacy policy aspect for each sensitivity level?
6) What options are available to define the purposes of privacy policy aspects?
7) What options are available to define the retention of privacy policy aspects?
8) What options are available to define the recipient of privacy policy aspects?
9) What options are available to define the obligation of privacy policy aspects?
10) What options are available to define the consent of privacy policy aspects?

4.2.2. Conceptualisation

Through this activity, eight concepts were identified based on the domain knowledge and represented as classes first, and then the relationships between classes were established. Finally, the properties, including data type properties and object properties, were defined for each class.

The eight concepts are listed in Table 3 along with the competent questions they are supposed to answer. The relationships between associated classes are illustrated in Fig. 1. The properties of each class, including the data type and object properties, are listed in Table 3.

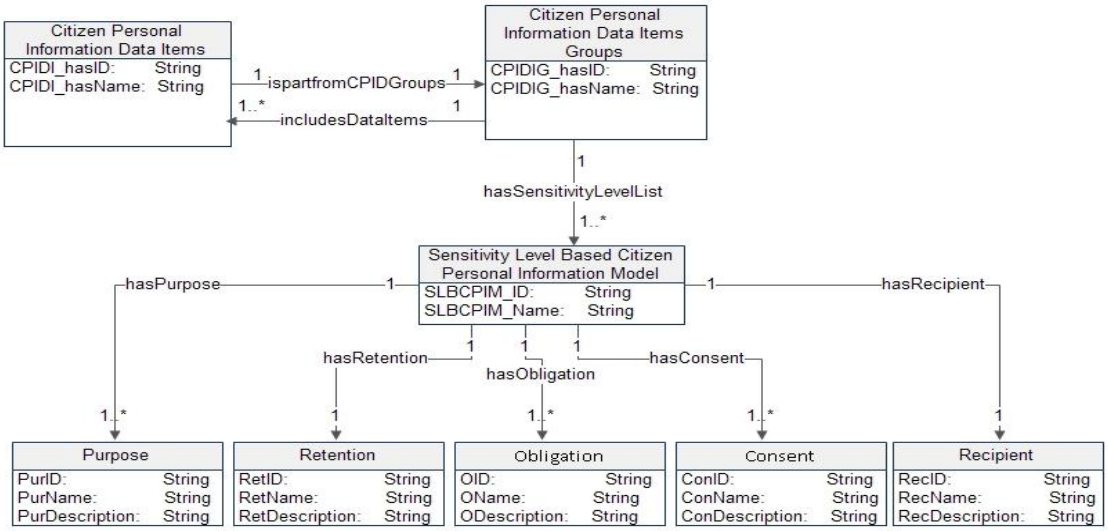

Fig. 1. The relationships between the classes in the SLBCPIM.

4.2.3. Formalisation and implementation

The ontology model developed in the conceptualisation must be implemented to be useful for applications. We choose Protégé-OWL as ontology development tool and OWL DL as the ontology development language. Protégé-OWL supports graphical representation of a class hierarchy though the OWLVIZ plug-in. Fig. 2 shows the hierarchy of SLBCPIM though the OWLVIZ plug-in.

4.3. Post-Development Phase: Evaluation

This phase aimed to evaluate the sensitivity level ontology (SLBCPIM) developed in the previous phase. The purpose of the evaluation was to ensure that the ontology was built correctly (verification) and according to certain specified ontology quality criteria (validation) [13]. Consequently, the evaluation was composed of two steps: ontology verification and ontology validation [14].

4.3.1. Ontology verification

For the verification, we aimed to check determine whether the ontology was built correctly. For this purpose, we employed two methods to verify the sensitivity level ontology (SLBCPIM) from different levels. The first method was to use the Manchester OWL validator to verify the SLBCPIM to ensure that the SLBCPIM conforms to the OWL2 DL profile. The verification result was satisfactory. The second method was to use Pellet, a Protégé built-in reasoner, to ensure that the following criteria were satisfied: 1) there was no contradictory concept that would be deduced from other concepts; 2) the ontology is complete in terms of disjointed knowledge and the classification hierarchy; 3) the ontology is concise in terms of dispensable concepts and absolute prolixity between concepts and 4) there are no unwanted subclasses, no repetitions of relations and no identical formal concepts of classes. The verification results were satisfactory.

4.3.2. Ontology validation

For the validation, we aimed to determine whether the ontology met the requirements, i.e., to check the

competency of the ontology to see whether the ontology can answer the competency questions [13]. For this purpose, we used SPARQL queries to extract answers to the competency questions listed in specification section and compared the extracted and expected results (the expected results were obtained from the domain experts). Table 4 shows examples about the SPARQL queries designed to answer the corresponding competency questions along with the figure number that shows the extracted query answer in the Fig. 3 and Fig. 4.

Table 3. Eight Classes with Related Competence Questions

Class name	Class description	Related competence questions	Citizen Personal Information Data Item Group Name (CPIDIG_Name)	Citizen Personal Information Data Items (CPIDI_ID)
Citizen Personal Information Data Groups Class	This class describes the information groups that contain items having the some sensitivity levels. It includes CPIDGs' options and specifies CPIDIs for each group.	Question 2 and Question 3	CPIDI_hasID CPIDI_hasName	ispartfromCPIDGroups
Citizen Personal Information Data Items Class	It is defined as collections of CPIDIs.	Question 1	CPIDIG_hasID CPIDIG_hasName	hasSensitivityLevelList includesDataItems
Sensitivity Level Based Citizen Personal Information Model Class	It includes multiple subclasses to define set of levels for each group of CPIDI and specifies privacy-related aspects for each level, such as obligation, consent, purpose, retention and recipient.	Question 4 and Question 5	SLBCPIM_hasID SLBCPIM_hasName	hasPurpose hasRetention hasRecipient hasObligation hasConsent
Obligation class	This class describes the complementary actions that need to be performed by the system	Question 9	hasOID hasOName hasODescription	
Consent class	This class describes the established agreement between the systems and citizens regarding usage of data that are different from its consented purpose by authorized people	Question 10	hasConID hasConName hasConDescription	
Purpose class	This class describes the reason for using data.	Question 6	hasPurID hasPurName hasPurDescription	
Retention class	This class describes the periods of time that a citizen's personal information should be kept.	Question 7	hasReteID hasReteName hasReteDescription	
Recipient class	This class describes the entities/agents that receive the citizen's personal information.	Question 8	hasRecID hasRecName hasRecDescription	

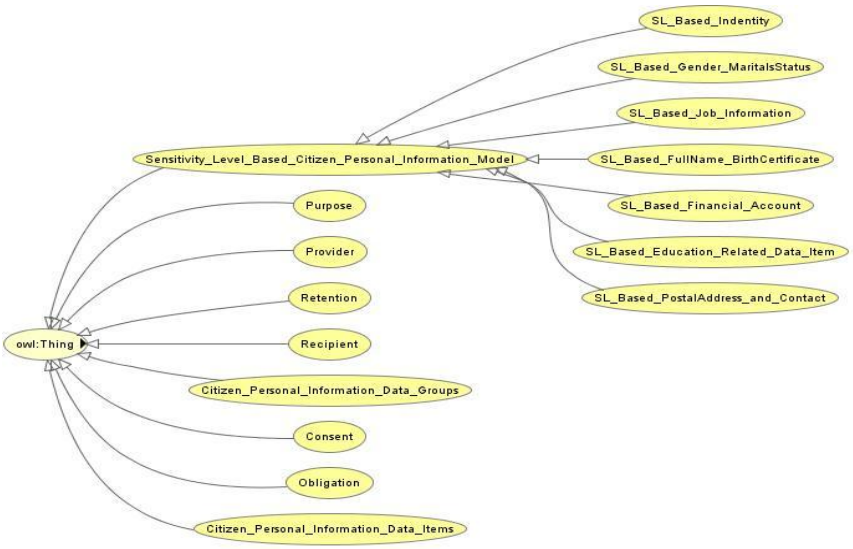

Fig. 2. Hierarchical structure of concept classes.

items in the context of e-government services. For ease of management, the citizen personal information in the context of e-government services is classified into seven groups, such as the identify information group and the job information group. Each group of data items has a number of sensitivity levels, determined based on common sense and survey results and available for citizens to choose for their personal data items in the group. For example, for the identify information group, there are three sensitivity levels, and a citizen can choose a level for his or her identify information data items, such as driver's license number (ID used in Australia) or Social Security number (ID used in Saudi Arabia). Each sensitivity level corresponds to a privacy policy that has pre-defined aspect options. These options will be guaranteed in e-government systems to satisfy citizens so that they can feel safe when they use e-government services.

In this section, we present the case of using the SLBCPIM to extract required information to set up privacy preferences for citizens' personal information items. This model is used to find the appropriate sensitivity levels for citizens' personal data items and the corresponding privacy policy aspect options.

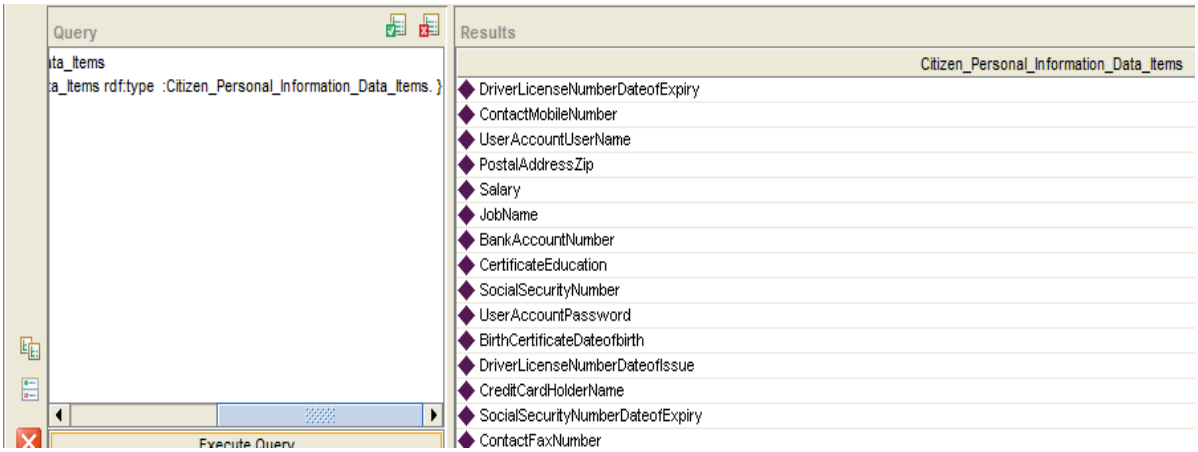

Fig. 3. SPARQL query with answer for competency question 1.

Table 4. The Validation Task

Competence Questions	SPARQL query SPARQL	query's answer
1. What are citizen personal information items (CPIDI) in the context of using e-government services?	SELECT ?Citizen_Personal_Information_Data_Items WHERE {?Citizen_Personal_Information_Data_Items rdf:type :Citizen_Personal_Information_Data_Items. }	Fig. 3
2. What are citizen personal information groups (CPIDIG)?	SELECT ?Citizen_Ppersonal_Information_Groups WHERE {?Citizen_Ppersonal_Information_Groups rdf:type :Citizen_Personal_Information_Data_Groups. }	Fig. 4

4.4. Case Description

Life events are used to integrate multiple e-government services and the life events use citizen personal information data items (CPIDI) to complete apply life event. In our case, there are two examples of life events: the Saudi Arabia King Abdullah Scholarship Program (SAKASP LE) and the Hafiz Program (Hafiz LE). These examples are related to the Saudi government. In these examples, different CPIDIs are used by the SAKASP LE application and the Hafiz LE application. This means that there are different CPIDIs when citizens apply the life events and different sensitivity level options for each CPIDI based on its related group.

In this case, the applicant has different levels of sensitivity when he or she needs to disclose his or her personal information. These levels range from a low level.

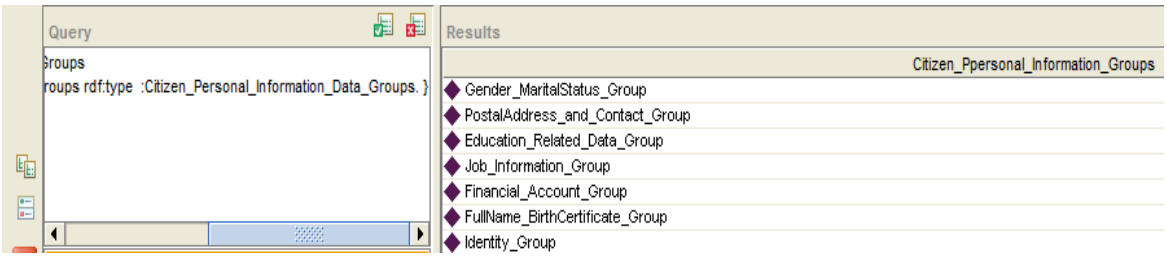

Fig. 4. SPARQL query with answer for competency question 2.

```
Query 1:
SELECT  ?Citizen_Personal_Information_Data_Items
?Citizen_Personal_Information_Data_Groups
WHERE { ?Citizen_Personal_Information_Data_Items
:ispartfromCPIDGroup
?Citizen_Personal_Information_Data_Groups.
?Citizen_Personal_Information_Data_Items
:CPIDI_hasName[given data item]. }
```

Fig. 5. SPARQL query to extract the data group for a given data item.

```
Query 2:
SELECT  ?Citizen_Personal_Information_Data_Groups
?SL_Based_Indentity
WHERE {
?Citizen_Personal_Information_Data_Groups
:hasSensitivityLevelList ?SL_Based_Indentity.
 ?Citizen_Personal_Information_Data_Groups
:CPIDIGroup_hasName [given data group]. }
```

Fig. 6. SPARQL query to extract the sensitivity level for a given data group.

5. Application of SLBCPIM—A Case Study

The SLBCPIM is a knowledge base of the sensitivity degrees of citizen personal information data items in the context of e-government services. For ease of management, the citizen personal information in the context of e-government services is classified into seven groups, such as the identify information group and the job information group. Each group of data items has a number of sensitivity levels, determined based on common sense and available for citizens to choose for their personal data items in the group. For example, for the identify information group, there are three sensitivity levels, and a citizen can choose a level for his or her identify information data items, such as driver's license number (ID used in Australia) or Social Security number (ID used in Saudi Arabia). Each sensitivity level corresponds to a privacy policy that has pre-defined aspect options. These options will be guaranteed in e-government systems to satisfy citizens so that they can feel safe when they use e-government services.

In this section, we present the case of using the SLBCPIM to extract required information to set up privacy preferences for citizens' personal information items. This model is used to find the appropriate sensitivity levels for citizens' personal data items and the corresponding privacy policy aspect options.

5.1. Case Description

Life events are used to integrate multiple e-government services and the life events use citizen personal information data items (CPIDI) to complete apply life event. In our case, there are two examples of life events: the Saudi Arabia King Abdullah Scholarship Program (SAKASP LE) and the Hafiz Program (Hafiz LE). These examples are related to the Saudi government. In these examples, different CPIDIs are used by the SAKASP LE application and the Hafiz LE application. This means that there are different CPIDIs when citizens apply the life events and different sensitivity level options for each CPIDI based on its related group.

In this case, the applicant has different levels of sensitivity when he or she needs to disclose his or her personal information. These levels range from a low level (when the applicant is not much concerned about the privacy of his or her personal information) to a high level (when the applicant is a very conservative person who sets the sensitivity levels at the high end). For example, when applicant A needs to apply to the SAKASP LE, it can include various levels of sensitivity: a low level when applicant A is not much concerned

about the privacy of some CPIDIs, such as gender, a moderate level when applicant A is moderately conservative with some CPIDIs, such as date of birth and a high level when applicant A is very conservative with some CPIDIs, such as Social Security number.

Table 5. Data Items with Data Group and Sensitivity Levels

CPIDI	CPIDIG_ID	Sensitivity level options
Social Security Number	Identity Information	SL_Based_Identity_L1 SL_Based_Identity_L2 SL_Based_Identity_L3
Full Name	Birth Information (including Full Name)	SL_Based_Full_Name_Birth_Certificate_L1 SL_Based_Full_Name_Birth_Certificate_L2 SL_Based_Full_Name_Birth_Certificate_L3 SL_Based_Full_Name_Birth_Certificate_L4
Date of birth		

5.2. Life Event Cases and the Needed CPIDIs

Base on the case description, there are different CPIDIs for each life event. In addition, there are different sensitivity levels for each CPIDI based on its related CPIDIG. Therefore, this section summarizes the CPIDIs for each life event case; for example, SAKASP LE application includes Social Security Number, Full Name and Date of birth, etc.

5.3. Sensitivity Levels for Each CPIDI

For each CPIDI, the data group that this item belongs to needs to be extracted, and then the sensitivity level for this data group will be extracted. The SPARQL query to find the data group for a given data item is shown in Fig. 5 and referred to as Query 1.

The SPARQL query to extract the sensitivity level set for a given data group is shown in Fig. 6 and referred to as Query 2.

Using the Queries 1 and 2, the groups and corresponding sensitivity levels for each CPIDI can be extracted. The examples about results are listed in Table 5.

Query 3:
SELECT ?purpose
WHERE { ?SL_Based_Indentity :hasPurpose ?purpose.
?SL_Based_Indentity :SLBCPIM_hasName [*given sensitivity level*].}

Query 4:
SELECT ?recipient
WHERE { ?SL_Based_Indentity :hasRecipient ?recipient.
?SL_Based_Indentity :SLBCPIM_hasName [*given sensitivity level*].}

Query 5:
SELECT ?consent
WHERE { ?SL_Based_Indentity :hasConsent ?consent.
?SL_Based_Indentity :SLBCPIM_hasName [*given sensitivity level*].}

Query 6:
SELECT ?obligation
WHERE { ?SL_Based_Indentity :hasObligation ?obligation.
?SL_Based_Indentity :SLBCPIM_hasName [*given sensitivity level*].}

Query 7:
SELECT ?retention
WHERE { ?SL_Based_Indentity :hasRetention ?retention.
?SL_Based_Indentity :SLBCPIM_hasName [*given sensitivity level*].}

Fig. 7. SPARQL queries for extracting policy aspects for a given sensitivity level (Query 3).

5.4. Citizen Sets up His or Her Comfortable Sensitivity Level for Each Data Item

When a citizen applies to the SAKASP LE, he or she needs to set up comfortable sensitivity levels for the CPIDI needed in the application. This section shows examples of CPIDIs using the SAKASP LE application and the sensitivity level options for each CPIDI. Those options range from a low level, 'Level 1' to a high level. For example, Social Security number (SSN) includes three options which are level 1, level 2 and level 3.

5.5. Privacy Policies for the Data Items in Terms of Privacy Aspect Options

When using e-government services, a citizen has an opportunity to set up his or her privacy policy for each personal information item. A privacy policy consists of five aspects, purpose, recipient, consent, obligation and retention, and each aspect has a few options (see Table 1). Thus, each privacy policy has five aspect options, and each option corresponds to one aspect. Each sensitivity level corresponds to a specific policy, and this policy can be extracted based on the given sensitivity level.

The SPARQL queries to extract the privacy policy aspects for a given sensitivity level are shown in Fig. 7 and referred to as Queries 3–7, respectively.

Example about using queries 3–7, the privacy policies based on a selected sensitivity level for social security number can be found. The results are listed in Table 6.

Through this case study, it can be seen that the SLBCPIM can be used to set up privacy preferences for citizen personal information items with ease and convenience.

Table 6. Privacy Policies for Sensitivity Levels

CPIDI	Sensitivity level options	Purpose	Retention	Recipient	Obligation	Consent
Social Security number (SSN)	Level 1	Citizen Request Administrator Profile	Retention Time	Ours	Delete after Use Notification	No Consent
	Level 2	Citizen Request Profile	Retention Time	Ours	Delete after Use Notification	No Consent
	Level 3	Citizen Request Administrator	Retention Time	Ours	Delete after Use Notification	No Consent

5.6. Privacy Preference-Setting Interfaces

In this section, we present Interfaces for privacy preference settings. To integrate the SLBCPIM with the system and design the interface, we use Eclipse as a Java editor, the Jena framework and the SPARQL query language. A complete explanation of the Jena framework and the SPARQL query language are beyond the scope of this paper, but further information on how to use the Jena framework with the SPARQL query language to consume ontologies can be found at http://Jena.apache.org/ and http://www.w3.org/TR/rdf-sparql-query/. These languages and framework can support to consume SLBCPIM to help users when they need to set up and save their privacy preferences.

To navigate the privacy preference settings page as shown in Fig. 8, the user can click on the Privacy Preference Setting Button on the citizen home page. When the system loads the privacy preferences setting page, the system will load the SLBCPIM.owl file. The life event section, CPIDIG section, CPIDI section and privacy policy section use SLBCPIM.owl to extract life event instances, CPIDIG instances, CPIDI instances and privacy policy instances using the Jena framework and the SPARQL query language.

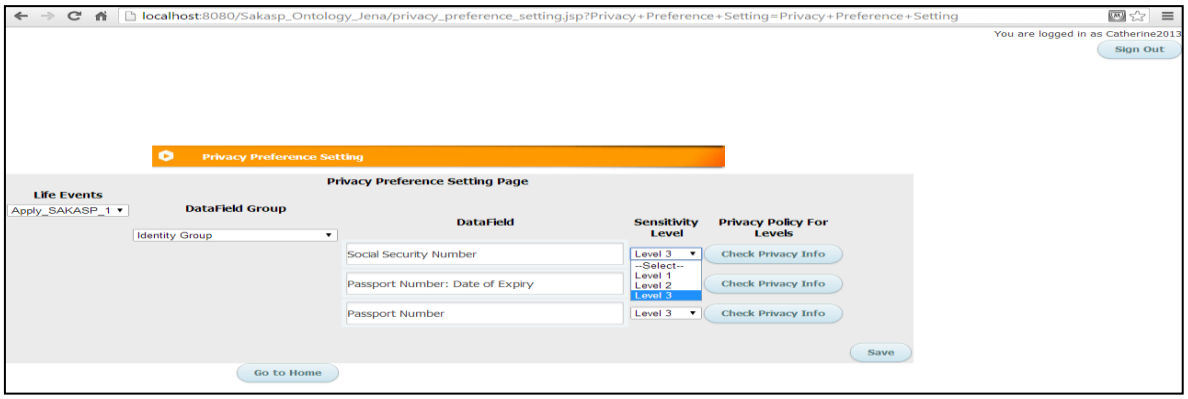

Fig. 8. Privacy preference setting screen 1.

When user selects desired life event, on selection of life event browser makes an AJAX request to pull the related CPIDIG and CPIDI from Server(PrivacyPreferencetInfo.java Class) with life event as a parameter as shown in Fig. 8. After successful response, user can see CPIDIG select and can select desired group to see its related CPIDIs and other default details related to respective such as Sensitivity level and Privacy Policy level descriptions as shown in Fig. 8.

In addition, server queries the database to obtain the default (or a selected) level by using the UserID CPIDIG_ID, SLBCPIM_ID and CPIDI_ID parameters. User can view respective privacy preference by clicking Check Privacy Info button .It present info in new Modal window as shown in Fig. 9.

In addition, the user can change the sensitivity level for his or her CPIDI as shown in Fig. 8. When the user selects another sensitivity level, the privacy policy related to the selected sensitivity level will be extracted from SLBCPIM by using the Jena framework and the SPARQL query language.

Finally, the user can click on the Save button to update the privacy preferences related to the life event CPIDI. Engine calls a servlet and saves the data to the citizen_privacy_preference table in the citizen_privacy_preference_database database (MySQL db). Engine returns a success message or a fail message.

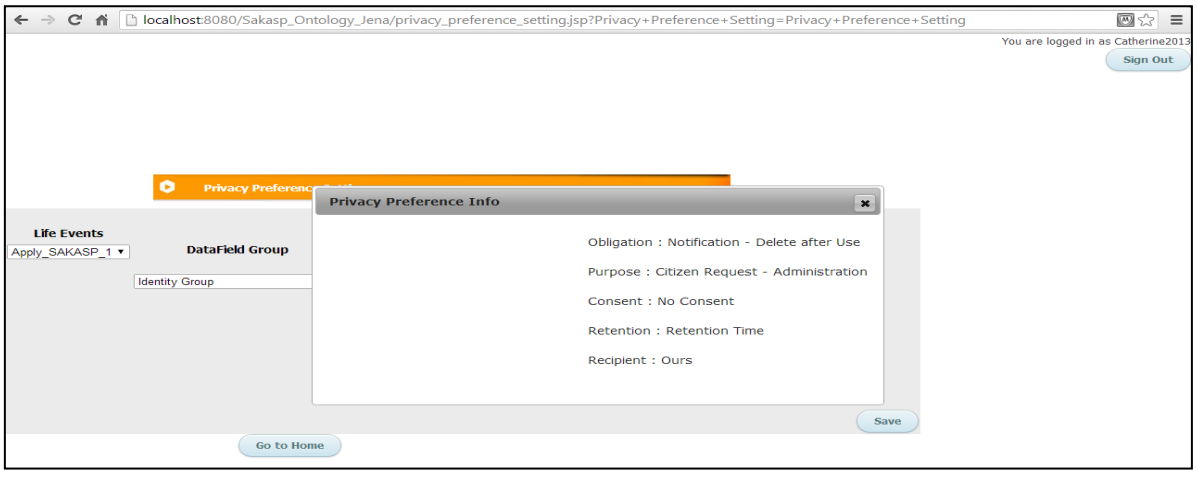

Fig. 9. Privacy preference setting screen 2.

6. Discussion and Conclusions

Over time, the development of information technology will affect the collection of citizens' personal information with consequences that are potentially both beneficial and harmful to individuals. At the same time, the development of a privacy model can improve the acceptance of e-government services. Concerning these two points, this paper has considered the protection of citizens' personal information in the

e-government service domain. Specifically, this paper developed a SLBCPIM model to support citizens in specifying their privacy preferences in the context of using e-government services.

The findings of this study are in line with existing studies showing that an ontology has potential benefits in enforcing privacy protection. This study is different to some degree from other studies in the sense that other studies have proposed solution-based ontologies to develop security issues and access control rather than focus on citizens to give them opportunities to control their privacy preferences. The case study shows that the SLBCPIM can effectively support citizens in specifying their privacy preferences regarding sensitivity levels for their personal information.

Future studies will focus on the implementation of policy aspect options to guarantee security so that citizens will feel safe and confident in providing their personal information to e-government service agencies.

Acknowledgment

The authors wish to express their special thanks to all the participants. Also, the authors are grateful to the anonymous reviewers for their valuable comments and suggestions to improve the presentation of this paper. This work has been supported by Center for Quantum Computation and Intelligent Systems (QCIS) of Faculty of Engineering and Information Technology at University of Technology Sydney, Australia.

References

[1] Alqahtani, A., Lu, H., & Lu, J. (2010). Towards semantic-aware and ontology-based e-government service integration–An applicative case study of Saudi Arabia's King Abdullah Scholarship Program. In G. Phillips-Wren, L. C. Jain, K. Nakamatsu, & R. J. Howlett (Eds.), *Advances in Intelligent Decision Technologies*, (pp. 403-411). Heidelberg: Springer.

[2] Chan, F., Thong, J. Y., Venkatesh, V., Brown, S., Hu, P., & Tam, K. Y. (2010). Modeling citizen satisfaction with mandatory adoption of an e-government technology. *Journal of the Association for Information Systems*, *11*, 519-549,

[3] Cranor, L., Langheinrich, M., Marchiori, M., & Reagle, J. The platform for privacy preferences 1.0 (p3p1.0) specification. Retrieved June 20, 2002, from http://www.w3.org/P3P/.

[4] Paul, A., Satoshi, H., Günter, K., Calvin, P., & Matthias, S. Enterprise privacy authorization language (epal). Retrieved June 20, 2003, from http://www.zurich.ibm.com/security/enterprise-privacy/epal/Specification/index.html.

[5] OASIS. OASIS extensible access control markup language (XACML). Retrieved June 20, 2004, from https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml.

[6] Hecker, M., Dillon, T. S., & Chang, E. (2008). Privacy ontology support for e-commerce. *Internet Computing*, *12*, 54-61,

[7] Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum.

[8] Fensel, D. (2001). *Ontologies: Silver Bullet for Knowledge Management and Electronic Commerce*. New York: Springer,

[9] Isaza, G., Castillo, A., López, M., & Castillo, L. (2009). Towards ontology-based intelligent model for intrusion detection and prevention. In Á. Herrero, P. Gastaldo, R. Zunino, & E. Corchado, (Eds.), *Computational Intelligence in Security for Information Systems* (pp. 109-116). Berlin Heidelberg: Springer.

[10] Qin, L., & Atluri, V. (2010). Semantics-aware security policy specification for the semantic web data. *International Journal of Information and Computer Security*, *4*, 52-75,

[11] Fernández-López, M., Gómez-Pérez, A., & Juristo, N. Methontology: (1997). From ontological art

towards ontological engineering. *Proceedings of the Ontological Engineering AAAI-97 Spring Symposium Series*. Stanford University, EEUU.

[12] Gruninger, M., & Fox, M. (1995). Methodology for the design and evaluation of ontologies. *Proceedings of the Workshop on Basic Ontological Issues in Knowledge Sharing Held in Conjunction with IJCAI-95*. Montreal, Canada,

[13] Vrandecic, D. (2010). Ontology evaluation. PhD thesis, KIT Karlsruhe Institute of Technology, Karlsruhe, Germany.

[14] Gómez-Pérez, A., Fernández-López, M., & Corcho, O. (2004). *Ontological Engineering: With Examples from the Areas of Knowledge Management, e-Commerce and the Semantic Web*. Springer Verlag.

Abdullah A. Alqahtani is a Ph.D. candidate in information systems and the director of the Decision Systems and e-Service Intelligence Research Laboratory in the Faculty of Engineering and Information Technology at the University of Technology Sydney (UTS), Australia. In addition, Abdullah began his career at University of Dammam in Saudi Arabia, College of Computer Science and Information Technology, Dammam. His main research interests are in the area of e-government, e-service integration and privacy.

Hai Yan Lu is a senior lecturer at the Faculty of Engineering and Information Technology, University of Technology, Sydney and a core member of Centre for Quantum Computation and Intelligent Systems. Her main research interests include modelling and optimum design of electromagnetic devices, optimisation techniques, decision-making support systems in production planning for electric power markets.

Jie Lu is a professor at the Faculty of Engineering and Information Technology, University of Technology, Sydney and a core member of Centre for Quantum Computation and Intelligent Systems. Her main research interests include decision support systems, e-services, e-business, e-government, group decision making, resource planning, database design and development, system modeling, web-based information systems, intelligent decision support systems, fuzzy optimization, fuzzy decision making, business intelligence, personalised recommender systems and system evaluation.