Development of an E-Government ontology to support Risk Analysis

Onyekachi Onwudike, Russell Lock, Iain Phillips
Department of Computer Science, Loughborough University
o.c.onwudike@lboro.ac.uk
r.lock@lboro.ac.uk
i.w.phillips@lboro.ac.uk

Abstract: The complexity of governments is one of the biggest problems citizens face in engaging with them. This complexity is seen in the growing number of departments and services that a government is made up of and the need for citizens to interact with these departments or services independently. This research shows a lack of efficiency in the E-Government domain due to the vertical alignment of services and the need for complex collaboration across the departments, which all too often does not exist. We propose that an ontology could potentially help to foster interactions between departments and services, and thereby manage this complexity more efficiently. Although ontologies exist for different subject domains, the quality and suitability of these ontologies in the government domain at the present time gives rise for concern. Ontologies have the potential to play an important role in the design and development of government services. The key reason behind the development and design of an ontology for the E-Government domain is to use knowledge that is resident in the domain of governments to reduce risks associated with the delivery, combination and dependencies that exist amongst services so that the resilience of the E-Government domain can be improved throughout government. This paper addresses the issue of identifying and analysing risk in the development and deployment of E-Government services. Relevant information on risks that may occur with respect to services can be collected, compiled and disseminated which can serve as prediction tools for future governments as well as enable service providers make choices that would enable them fulfil service requirements adequately. The aim of this research is to contribute by constructing an ontology that is aimed at gauging the risks associated with using solutions across departments and even governments. Further, we also document how we have made use of queries to validate this ontology.

Keywords: E-Government, Ontology, Relationships, Reuse, Risks

1. Introduction

As a working approximation the average government is made up of around 50-80 different departments and agencies. For matters that are as simple as registering the birth of a child, different agencies and departments require a bewildering array of information often inputted in different ways, into different systems, and stored/accessed in multiple locations. Rather than these departments communicating amongst themselves, they expect citizens to communicate with them individually. One solution to the problems faced by governments is the use of ontologies. The reasons for building E-Government ontologies are many and varied. They include but are not limited to the following:

1. To create and distribute information;
2. To maintain information on data and its usage adequately;
3. To enforce standards in the way data is exchanged;
4. To aggregate data with the use of languages such as OWL;
5. To interpret data formally with the use of semantics and to adequately control
6. vocabularies;
7. To emphasize trust in data sources because there is provenance of information;
8. To compare and correlate data;
9. To make government efficiencies and effectiveness transparent; and
10. To make sure there is accountability in the process of making policies.

Sowa (Sowa 2000) defined an ontology as a discipline that forms part of the field of knowledge representation. Ontologies are commonly applied to model information from different application domains in order to support analysis. They can be used in the representation of services governments offer to her citizens as well as in supporting the providers of these services in the delivery of these services, and the receivers of these services in accessing the availability of services to them in a structured and logical way. Different E-Government ontologies have been developed for different strata of government in the past; however, these ontologies

have had little or no impact on E-Government as a whole arguably due to the lack of collaboration that has taken place during construction, and due to the inherent lack of collaborative support built into them by the developers. Therefore the ontology this paper presents has been explicitly designed to improve collaboration, and has been formulated using real world data. Although the idea of reuse across ontologies seems to be a welcome idea with respect to the problem of interoperability, the risks and disadvantages associated with reusing existing solutions, as well as making certain functionalities shareable between E-Government services is a concern. We explore the use of ontologies in overcoming risks associated with reusing solutions developed for one department in another department and conclude, with the support of case studies for evaluation, that the use of ontologies could be beneficial in gauging the risks associated with this. This theory is supported by a case study which highlights what can be achieved through reasoning with an OWL ontology extended appropriately by rules. The application aims at modelling the definition of risks that may be identified in the combination of services in the E-Government domain. Simplified examples are provided in the paper to illustrate why OWL needs to be supplemented with rules for reasoning over hybrid knowledge and potential issues with doing so are discussed.

The development of a suitably designed ontology could add value to the E-Government domain in areas of modelling relationships that exist between Departments and services as well as in overcoming the risks associated with reusing solutions across departments in government. Therefore, the role of the research and the artefact created in the form of an ontology is to educate governments and the providers of services so that risks can be reduced as well as the resilience of the system increased.

The rest of the paper is structured as follows: Section two elaborates on existing E-Government ontologies; Section three presents application contexts where a suitably designed ontology can be used to gauge risks in the E-Government domain; Section four makes use of instances of the E-Government ontology to present cases for its relevance and finally Section five presents the conclusions, limitations and potential of this novel approach.

2. E-Government Ontologies

In terms of the sharing of knowledge, an ontology is defined as an explicit specification of a conceptualisation (Gruber 1993). In computing, an ontology can be likened to a framework used for the representation of concepts (things, or ideas about things) and the relationships that exist between those concepts (Uschold & Gruninger 1996). Therefore an ontology is aimed at modelling only those entities and relationships deemed relevant within a particular domain. An E-Government ontology can be defined as an explicit description of the E-Government domain containing a common vocabulary to support shared understanding between users. Concepts and relations managed by any scientific community can benefit from formal definitions and the use of ontologies is one of the key ways to achieve this. Several E-Government ontologies have been developed in the past, including SmartGov, EGov, OntoGov, TerreGov etc.

While the OntoGov ontology focussed on making electronic services interoperable and accessible to people all over the globe it lacked the ability to specify roles and actors in the development of the ontology as well as the ability to logically make queries. The SmartGov ontology was designed with the intention of helping public authorities overcome barriers in planning, designing, and delivery of electronic services, but fell short because it was difficult to establish concepts that were related to E-Government in the ontology. Although the TerreGov ontology dealt with interoperability issues of E-Government services for local and regional governments there was an absence of focus for a global community. The EGov ontology encouraged a one-stop government and provided information to citizens but lacked the ability to define complex concepts and relationships; The focus of the QUALEG and QUONTO ontologies was on the problem of integrating services but failed to establish interaction between government and her citizens. Therefore citizens perception of government services were ignored. The question therefore arises, why are the ontologies previously developed not being applied today? Although there was an attempt by these ontologies to address varying problems in the E-Government domain, (Gugliotta A et al. 2005) argue that not one of these ontologies embraces Semantic Web technologies to represent concepts and actions. Many of these ontologies are already obsolete and more crucially lack semantic consistency in their design which has led to loss of critical information. Despite this, ontology development for Electronic Government is an area that has received considerable interest. According to (Fonou-dombeu & Huisman 2011), ontologies are used to describe and specify E-Government services (E-services), primarily because semantic integration and interoperability of E-

services are facilitated with their use; there is ease in composition, matching, mapping and merging of various E-Government services. Therefore the purpose of the E-Government ontology is to facilitate adequate understanding of the E-Government domain by service providers so that issues relating to the integration of services as well as the risks associated with integration in the Government domain can be addressed, as well as used as prediction tools for future governments. It is extremely difficult to develop a single ontology that satisfies all users especially in the areas of precision, coverage, actuality and individualization. This can be attributed to the fact that specific approaches as well as vocabularies are needed by different departments for solving tasks specific to them (Stumme et al. 2000).

The development of E-Government ontologies in isolation, without wider integration in perspective and the lack of reuse of components present serious challenges for the E-Government domain. Ontologies serve as a platform or a means for defining the services offered by governments and attempts have been made at the development of E-Government ontologies. The use of ontologies for knowledge representation can enhance organizational communication and re-usability, and serve as the building blocks for intelligent systems.

To the best of our knowledge, there is no directly related work focussed on the development of an E-Government ontology to gauge risks associated with E-Government services. The focus of other related work have been on the development of semantic driven government (Fonou-dombeu & Huisman 2011). (Gugliotta et al. 2005) focussed on the development of E-Government portals and (Sheng & Lingling 2011) focussed on the application of ontology in E-Government.

2.1 Method of Development

To develop the E-Government ontology used in this paper, the steps provided by (Noy & McGuinness 2001) were followed with emphasis on the repetitive process stated in it. This method of ontology development as proposed by (Noy & McGuinness 2001) was used because it is an increasingly popular method for organizing information and has successfully been used in the past by other ontology developers. The process involved determining the scope and domain of the ontology which involved sketching a list of questions the ontology should be able to answer referred to as competency questions; enumerating important terms and relationships; definition of classes and subclasses as well as formulating a class hierarchy; definition of class properties as well as their cardinalities and values and creating instances in the ontology. The competency questions are focussed on what we intend the ontology to do and what questions the ontology should be able to address. With the help of the competency questions we were able to formalise a scope for the ontology which aided the enumeration of important terms and enabled us to define the class structure of the ontology. The key competency questions that were considered during the development of the ontology include but are not limited to the following:

1. What services are available to a citizen?
2. What service is characteristic of a department?
3. What services can be combined?
4. What are the criteria for combining services?
5. What happens if services that are combined fail?

Based on this list of questions, the ontology will include the information on various services, departments and their characteristics.
The design of the ontology was carried out generically so that it could be used to support reuse across governments globally. A large number of related terms were gathered from existing publicly available documentation with the most general and most important of them forming the classes; some of them were used to form properties and others were not used at all because their relevance in the ontology could not be ascertained. Development of the classes and the corresponding class hierarchy formed the next stage of the process. Considering that different approaches can be used in developing the class hierarchy which are the top-down approach, the bottom-up approach and a combination of the two approaches we made use of a combination of the two approaches. In response to the competency questions, we made use of a combination of both approaches because the top-down approach was best suited which gave a well-defined class hierarchy and then the remaining concepts were incorporated into the ontology with the bottom-up approach. The development of the class hierarchy paved the way for definition of class and objects properties which included

defining values, value types and their cardinalities. In order to highlight different scenarios of risks, we made use of the UK Government website as our source of data because it contains semi-structured data and because of the mode of storage of data. The UK Government is one that works with devolved ministries, emergency responders and other organisations which enables the UK government to prepare for, respond to and recover from risks it is faced with. Therefore, in order to achieve this there has to be a preparation and readiness to deal with risks and emergencies not just from the stakeholders point of view but also in terms of the flexibility of an ontology to support the evolving nature of services and situations. We defined services in terms of other services they were dependent on; departments in terms of departments they were dependent on and were able to model and analyse situations where a given department were critically dependent on another for systems leading to potential shared points of failure. A typical example of departments being dependent on other departments included in our ontology from the UK Gov website is the Attorney General's Office which is a Ministerial department that works with three Non-Ministerial Departments (Crown Prosecution Service, Serious Fraud Office and the Treasury Solicitors Office)and an agency (HM Crown Prosecution Service Inspectorate). Based on the way the UK Government has been structured, it is clear that certain departments cannot function without some other departments or agencies being in place. It also shows that since some departments are overly dependent on other departments, there could be overlooked or incorrectly calculated risks present. This therefore highlights the need to address actively whether reuse is desirable, and whether the details and potential implications of that reuse are clearly defined within government.

In terms of services being dependent on other services but still functioning largely in silos we highlight a scenario based on the UK Benefits Service. Child Benefit is a type of generic Benefit service in terms of our ontology, which itself is represented in this scenario by the creation of a specific instance of that service within the UK government, the Guardians Allowance Service. However, the Guardians Allowance Service is also an instance of the Deaths and Benefits Service which is also a type of Benefit. Other examples include the Carers and Disability Benefit service a type of Benefit service also which shares Carers Credit as an instance with the Job Seekers Allowance service and the Low Income Benefits service. We see the dependencies between these services and conclude that while these dependencies may have been considered in terms of risk, an ontology would make such a process more efficient by structuring the data logically.

In Figure 1 we show a part of the developed ontology hierarchy. The classes of the depicted ontology, i.e. E-Government, Person, Threats etc. and their corresponding subclasses which cover the basic concepts that describe the context of an E-Government application. In terms of the structure of our ontology and to overcome the problems other E-Government ontologies faced which included a surprising lack of semantic consistency and insufficiently defined relationships between the different departments; we developed our structure thus:

The set of government services is primarily considered in terms of those users who have a relationship to the services, represented within our ontology by the class Person who can belong to a department and, offer, support or consume services. The structure of our ontology also helped us define relationships beyond the ‘is-a’ relationship commonly found in upper level ontologies.

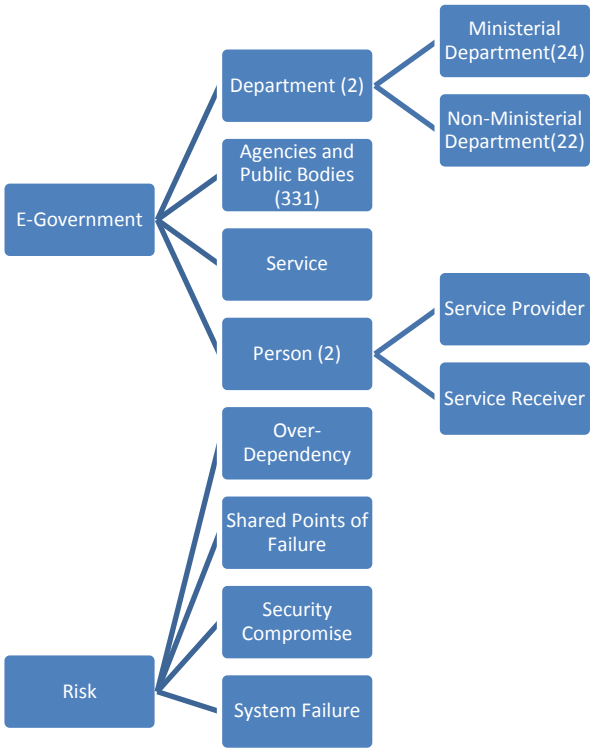

Figure 1: The ontology hierarchy

3. Application Scenarios

The purpose of E-Government is to provide services that are focussed on citizens as well as address the demands of citizens and businesses so that they can be accessible, responsive, simple and transparent for the users (Karyda et al. 2006). E-Government services are provided through applications that need to have increased security and privacy features. Although the security and privacy features are key to any government, the possibility of sharing services and reusing solutions across departments and even government cannot be ignored.

3.1 Benefit Service

In this section, we revisit the scenario of a Benefits service running in the UK E-Government domain (www.gov.uk). This service includes the different types of benefits accessible to citizens; when and how benefit payments are made; eligibility for benefits and when it is supposed to stop. The receiver of this service would be able to ascertain whether he is eligible for a benefit. The benefit issuing authority would be in a position to verify eligibility, make cross-checks and get additional information from the benefit credit facility. Although this process requires confidentiality, privacy and integrity of the entire benefit process; many of the features required are common to other departments or services such as the Births, Deaths, Marriages and care department. However, this scenario can be made up of the following processes but not limited to:

- Management of personal information by users
- Viewing of previous benefits received by users
- Processing of eligibility criteria
- Notification by system that additional information is needed
- Users update additional information required by system with the needed information.

Although in the scenario analysed, major security requirements need to be met such as authentication and authorization of users, this information needs to still be shared across departments requiring this information.

3.2 Births, Deaths and Marriages Service

In this section we present another scenario in the form of the UK Births, Deaths and Marriages service that offers the child benefit service as a subclass and yet has this same service as a type of service in the Benefits service (www.gov.uk). In the development of a Births, Death and Marriage application, this service includes the registration of a birth, death or marriage; eligibility for benefits and when it should stop; dealing with benefits, taxes and leaving care. This shows us that a solution used for the benefits department with respect to eligibility for benefits and when it should be stopped could be reused for the Births, Deaths and marriages department, however, the purpose of the ontology in this respect would be to highlight the risks related to doing so.

4. Using the E-Government ontology to gauge risks

In this section, we illustrate how the E-Government ontology can be used to gauge the risks associated with combining services or even reusing solutions. We also illustrate how the ontology is validated as development of the ontology progresses. We made use of Protégé4.2 for the development of the ontology and queries were run with the Racer reasoner. Protégé 4 is an ontology editor used for creating OWL ontologies. It cannot work without the OWL API in place. It makes use of a Description Logic Reasoner which checks the consistency of the ontology and automatically computes the ontology class hierarchy. For the purpose of this Research, we made use of OWL-DL which is known to be a more expressive OWL language. It is based on Description Logics which are a component of First Order Logic and are key to automated reasoning. It has the capability of computing the classification hierarchy of an ontology as well as checking for inconsistencies in the ontology (Horridge, 2007). The Racer Reasoner is used for making references and for answering queries over RDF documents (Gmbh 2010). We used it to check for inconsistencies in the ontology and to submit queries so that their validity could be verified. These queries we expressed with the use of the new Racer Query Language (nRQL). The nRQL is a query language that makes use of description logic for retrieving individuals from the A-box which is known as a set of assertions about individuals. This language allows the use of variables which are bound against the individuals in the a-box that satisfy the conditions. Protégé and Racer were able to communicate because of the RQL tab plug-in that was installed. We provide a set of nRQL queries with their answers below illustrating the use of the E-Government ontology to gauge risks associated with reusing solutions.

4.1 Results of nRQL queries

An ontology is said to be useful when it can give answers that are consistent to real-world questions. In this section, we list a number of questions a service provider is likely to come up with when attempting to reuse solutions in the E-Government domain. Although these questions are not exhaustive, they indicate what the ontology can deal with and what level of reasoning it can cope with. We express each question as an nRQL query and present the result of the executed query. The questions presented in this section also guided us in the development of the ontology while the queries presented were used in validating our ontology.

4.1.1 Questions associated with reusing solutions

Having an understanding of the type of risk that may take place when services are combined or solutions are reused gives us an insight into the conflicts that may take place within the back office situation especially with respect to sharing of resources and information property rights. (Homburg et al. 2002) analysed the effects of resource dependence theory and information property rights theory stating the conflicts that could stem from such mixtures in the network. The development of services requires heavy reliance on the use of IT systems. (Woll et al. 2013) outlined a major challenge associated with this as lack of interoperability between different IT systems. Although a lot of research and industrial activities have focused on the feasibility of interoperability in the past, the problem still lingers. (Woll et al. 2013) also outlined how approaches have been mapped out on embracing interoperability but there is a lack of application in the industry. This they attributed to the high cost of linking many different IT systems and the data contained in them.

To successfully build a platform for E-Government to operate requires the collation of information from the different departments and parastatals that make up the government. Hence, there is a lot of replicated data as data collated for one department may be the same data collated across other departments even though the modes of collation or delivery may differ. A typical scenario seen while building this ontology from the UK Government website is in the department of Birth, Deaths, Marriages and Care which has Child Benefit as one of the services it offers and a replication of this same service in the Department Benefits. The question is this, why can't the Department for benefits make use of the already existing framework the Birth, Deaths, Marriages and Care department has? Is there the need for the user of the system to fill this information independently for each department? The following results analyse the data in the ontology to attempt to answer the queries posed, highlighting the perceived threats and risks emergent from the data. The results have been cut down slightly for the purposes of the paper and are therefore illustrative rather than exhaustive and are an indication of how inferencing could potentially help in the analysis of risks in the E-Government domain:

1. What are the typical objectives of a benefit service?

```
nRQL Query:          (retrieve (?obj) (?obj |Objective|))
nRQL Result:    (((?OBJ |Data_Confidentiality|))
                     ((?OBJ |Availability|))
                     ((?OBJ |Data_Integrity|))
                     ((?OBJ |User_Eligibility|))
                     ((?OBJ |User_Accountability|))
                     ((?OBJ |User_Non_Repudiation|))
                     ((?OBJ |Accuracy|)))
```

In order to answer this question, we first highlight the objectives of the Benefit service. This enabled the modelling of the goals of this service into the ontology.

2. Which assets are confidential in a benefit system?

```
nRQL                 (retrieve (?asset) (and
Query:          (|Confidentiality| ?threat
                     |is_threatened_by|) (?asset ?threat
                     |damaged_by|)))
nRQL                 (((?ASSET |Benefit_Data|))
Result               ((?ASSET |Personal_Data|))
                     ((?ASSET |Cryptographic_Keys|)))
```

In order to address the question of confidentiality in the Benefit service, we had to examine potential threats to the confidentiality of citizens. In doing so we first had to determine the possible threats to the confidentiality of citizens, and model the assets that may be compromised or damaged by them. So, in the case of confidentiality, we modelled that the confidentiality of a citizen may be threatened by, for example user errors, cryptographic keys disclosure or compromise etc.

3. What are the typical objectives of the Births, Deaths and Marriages service?

```
nRQL Query:          (retrieve (?obj) (?obj |Objective|))
nRQL Result:    (((?OBJ |Data_Confidentiality|))
                     ((?OBJ |Availability|))
                     ((?OBJ |Data_Integrity|))
                     ((?OBJ |User_Eligibility|))
                     ((?OBJ |User_Accountability|))
                     ((?OBJ |User_Non_Repudiation|))
                     ((?OBJ |Accuracy|)))
```

In order to answer this question, we first highlight the objectives of the Births, Deaths and Marriages services. This enabled the modelling of the goals of this service into the ontology.

4. Which assets are confidential in the Births, Deaths and Marriages service?

```
nRQL                    (retrieve (?asset) (and
Query:          (|Confidentiality| ?threat
                        |is_threatened_by|) (?asset ?threat
                        |damaged_by|)))
nRQL                    (((?ASSET |Benefit_Data|))
Result  :               ((?ASSET |Personal_Data|))
                        ((?ASSET |Cryptographic_Keys|)))
```

In order to address the question of confidentiality in the Births, Deaths and Marriages service, we had to examine potential threats to the confidentiality of citizens. In doing so we first had to determine the possible threats to the confidentiality of citizens, and model the assets that may be compromised or damaged by them. So, in the case of confidentiality, we modelled that the confidentiality of a citizen may be threatened by, for example user errors, cryptographic keys disclosure or compromise etc. Questions 1-4 show us that the Benefits service and Births, Deaths and Marriages service have the same objectives. Therefore, there is a potential for reuse between these services.

5. What happens to departments that are dependent on other departments for shared resources or information?

```
 nRQL           (retrieve (?dependency)
Query:  (|Department functionality| ?risk
                is_threatened_by|))
nRQL            (((RISK |Over_Dependence|))
Result: ((?RISK |System_Failure|))
                ((?RISK |Shared_Points_Of_Failure|))
                ((?RISK |Security_Compromise|))
                ((?RISK |Reduced_System_Reliability|))
                ((?RISK |End_Of_Service|))
                ((?RISK| Decommissioning _Of_Department|)))
```

In order to answer this question, a list of potential risks had to be developed and structured for the ontology some of which are highlighted in the example above including Over Dependence, System Failure, Shared Points of failure, Security of the system being compromised, the reliability of the system being reduced and even abolition of a department which could lead to the termination of the service or services offered by that department.

6. Which risks might compromise the functionality of a department?

```
nRQL            (retrieve (?risk)
Query:  (|Department functionality| ?risk
                is_threatened_by|))
nRQL            (((RISK |Over_Dependence|))
Result: ((?RISK |System_Failure|))
                ((?RISK |Shared_Points_Of_Failure|))
                ((?RISK |Security_Compromise|))
                ((?RISK |Reduced_Funding|))
                ((?RISK |Reputation_Damage|)))
```

In order to model this question into our ontology, we had to determine the risks that may hamper a department meeting its remit to provide functional services to her citizens, with the example above indicating Over Dependence, Security Compromise.

7. Which threats can compromise the anonymity of the users of the system when services are combined?

```
nRQL        (retrieve (?threat)
Query:      (|User_Anonymity| ?threat
            is_threatened_by|))
nRQL        (((?THREAT |Impersonation|))
Result:     ((?THREAT |Malicious_Code|))
            ((?THREAT |User_Error|))
            ((?THREAT |OS_Bugs|))
            ((?THREAT |Application_Bugs|))
            ((?THREAT |Terminal_Highjack|)))
```

As services are combined and solutions reused across governments, the anonymity of users may be compromised, and we have highlighted a subset of the threats that a user may face if this is the case.

8. Can countermeasures be put in place so that there is no impersonation in the systems that are combined?

```
nRQL        (retrieve (?citizens information)
Query:      (?Citizens Information |No_Impersonation| |address|))
nRQL        (((?Citizens Information |Identification|))
Result:     ((?Citizens Information |Authentication|))
            ((?Citizens Information |Audit_Trails|)))
```

The example above shows that for this example to prevent impersonation in combined systems, audit trails would be beneficial.

9. Can dependencies among services bring about inter-departmental co-operation?

```
nRQL        (retrieve (?dependency)
Query:  (|Inter-departmental co-operation| ?dependency|))
nRQL        (((? Co-operation |Optimized Results|))
Result:  ((?Co-operation |Increased_Communication|))
            ((?Co-operation |Cognitive_Complexity|))
            ((?Co-operation |Enhanced_Solutions|)))
```

Co-operation between departments foster partnerships and collaboration. This involves having joint goals and a reliance on departments to accomplish the goal. When concepts from an ontology are imported from other ontologies, the dependencies that exist among them are managed using the reproduction of concepts to be imported (Kozaki et al. 2007). In the same vein, when dependencies amongst services exist, they reproduce all definitions related to the concepts produced. Services that are delivered in silos take more time in problem resolution. This could involve sending a client to multiple locations and could lead to information that is incomplete or inaccurate.

5. In conclusion

In this paper, we have discussed the role of ontologies in the delivery of E-Government services, the advantages of reusing the components and solutions that cut across these services as well as the inherent risks and challenges that a government may face with reusing components. The use of ontologies provides an effective means of capturing, describing and exploiting knowledge in the area of E-Government with its rapidly evolving departments and services. We presented the use of a developed E-Government ontology in multiple areas of application in Electronic Government for gauging risks that may face a government in areas of reuse.
A major challenge faced in modelling the ontology is the fact that the E-Government domain is an expansive one and insufficient tools have been developed to date during the research to enable accurate curation of all relevant terms. Once further developed, and supported by a suitable set of user tools the testing of the ontology in a national setting, currently planned to be that of the Nigerian government will take place.

References

Fonou-dombeu, J.V. & Huisman, M., 2011. Semantic-Driven e-Government : Application of Uschold and King Ontology Building Methodology for Semantic Ontology Models Development. , 2(4), pp.1–20.

Gmbh, R.S., 2010. RacerPro Reference Manual Version 1.9.

Gruber, T.R., 1993. Toward Principles for the Design of Ontologies Used for Knowledge Sharing. , pp.907–928.

Gugliotta A, Cabral Liliana & Domingue John, 2005. Knowledge modelling for integrating semantic web services in e-government applications Conference Item.

Gugliotta, A. et al., 2005. A conceptual model for semantically-based e-government portals.No Title. In *1st International Conference on eGovernment ICEG*. Ottawa, Canada.

Homburg, V., Bekkers, V. & Rotterdam, N., 2002. The Back-Office of E-Government (Managing Information Domains as Political Economies) Center for Public Management The Dutch Setting : Networks of Governmental Organizations and The Political Economy of Information. , 00(c), pp.1–9.

Karyda, M. et al., 2006. An ontology for secure e-government applications.

Kozaki, K. et al., 2007. A Framework for Cooperative Ontology Construction Based on Dependency Management of Modules. , (November), pp.33–44.

Noy, N.F. & McGuinness, D.L., 2001. *Ontology Development 101: A Guide to Creating Your First Ontology*,

Sheng, L. & Lingling, L., 2011. Application of Ontology in E-Government. *2011 Fifth International Conference on Management of e-Commerce and e-Government*, pp.93–96. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6092638 [Accessed April 22, 2014].

Sowa, J.F., 2000. *Knowledge representation: logical, philosophical and computational foundations*, Pacific Grove, CA, USA: Brooks/Cole Publishing Co.

Stumme, G., Studer, R. & Sure, Y., 2000. Towards an Order-Theoretical Foundation for Maintaining and Merging.

Uschold, M. & Gruninger, M., 1996. Ontologies: Principles Methods and Applications. *Knowledge Engineering Review*, 11(2), pp.1–63.

Woll, R., Geißler, C. & Hakya, H., 2013. Modular ontology design for semantic data integration. , pp.3–6.