



Secure Access Control in Semantic Web-Based E-Government Systems

ضبط الوصول في أنظمة الحكومة الإلكترونية المبينة على الويب الدلالي

Sary Jouhara : Department of Web Sciences, Syrian Virtual University, Damascus_Syria.

Mohamad Aljnidi : Scientific Studies and Research Center, Damascus_Syria.

Corresponding: sary_123785@svuonline.com

Submitted date: 28 May 2025 - Accepted date: 22 June 2025.

ABSTRACT

The rapid growth of semantic web technologies has led to their widespread adoption in e-government applications, addressing challenges related to administrative heterogeneity. However, integrating semantic web techniques into these applications introduces security vulnerabilities, particularly in access control mechanisms. This research proposes a secure access control solution for semantic web-based e-government systems. The proposed approach enhances the Flat Role-Based Access Control (Flat RBAC) model by incorporating ontology-driven methodologies and semantic reasoning. Domain-specific ontologies were developed to model the information of participating government entities, while a centralized ontology was designed to precisely define user roles and permissions. By leveraging semantic web technologies such as RDF (Resource Description Framework), OWL (Ontology Web Language), and SPARQL (SPARQL Protocol and RDF Query Language), the system enforces access policies dynamically and with semantic flexibility. The solution utilizes Apache Jena Fuseki as a triple store to facilitate interoperability among government agencies while ensuring that unauthorized access is prevented through semantic-based authentication. Additionally, a reasoning engine is employed to infer implicit facts from existing data, enhancing query responses and logical inference capabilities. The system was qualitatively assessed based on standard e-government criteria, confirming its support for flexible policy updates, secure access control, and semantic interoperability. In conclusion, this study provides a robust access control framework for e-government environments, demonstrating significant improvements in data interoperability and security management. These findings pave the way for future research on optimizing system performance and extending the approach to advanced access control models such as Hierarchical RBAC and Constrained RBAC.

Keywords: E-Government, Semantic Web, E-Government Security, Semantic Web Security, Access Control.

المخلص

أدى النمو السريع لتقنيات الويب الدلالي إلى اعتمادها على نطاق واسع في تطبيقات الحكومة الإلكترونية، ما ساعد في معالجة التحديات الناتجة عن اختلاف بيئات العمل الإدارية وتعقيدها. ومع ذلك، فإن دمج أساليب الويب الدلالي في هذه التطبيقات يؤدي إلى ظهور ثغرات في أمن المعلومات، لا سيما في مجال ضبط الوصول وإدارة الصلاحيات. يهدف هذا البحث إلى اقتراح حل آمن لضبط الوصول في أنظمة الحكومة الإلكترونية المبينة على الويب الدلالي، مع التركيز على تحقيق التوازن بين الأمان والكفاءة التشغيلية. يستند الحل المقترح إلى تعزيز نموذج التحكم بالوصول القائم على الأدوار (Flat RBAC) من خلال إدماج منهجيات مدعومة بالأنطولوجيا والاستدلال الدلالي. جرى تصميم أنطولوجيات متخصصة لتمثيل معلومات الجهات المشاركة في الحكومة الإلكترونية وضبط الوصول إليها باستخدام أنطولوجيا شاملة لتحديد أدوار المستخدمين وصلاحياتهم بدقة، ودمج تقنيات الويب الدلالي مثل RDF و OWL و SPARQL لتنفيذ السياسات على نحو ديناميكي ومرن. جرى الاعتماد على مخزن الثلاثيات Apache Jena Fuseki لتحقيق التشغيل البيئي بين الجهات الحكومية المختلفة مع ضمان منع الوصول غير المصرح به عبر تقنيات مصادقة مبينة على الأنطولوجيا. كما جرى تفعيل محرك استدلال لاستنتاج حقائق إضافية ما يعزز الاستجابة للاستعلامات واستخلاص المنطق. أُجري تقييم نوعي للنظام بناءً على معايير متعارف عليها في الحكومة الإلكترونية، وأظهرت النتائج أن النظام يدعم تحديث السياسات بمرونة، ويعزز الأمان، ويحقق قابلية التشغيل البيئي وقابلية التوسع. يفتح هذا البحث آفاقاً لأبحاث مستقبلية تهدف إلى تحسين الأداء، وتعزيز قدرات الاستدلال، وتوسيع النموذج ليشمل التحكم المتقدم بالوصول مثل Hierarchical RBAC و Constrained RBAC في بيئات واسعة النطاق.

الكلمات المفتاحية: الحكومة الإلكترونية، الويب الدلالي، أمان الحكومة الإلكترونية، أمان الويب الدلالي، ضبط الوصول.

INTRODUCTION

In recent years, the digital transformation of government services has emerged as a critical global priority. Nevertheless, e-government remains an active and evolving research field, as many coun-

tries have only implemented partial solutions and continue to face unresolved technical and organizational challenges. As stated in [1], "the development of a shared e-government knowledge base is

one of the key challenges of many e-government strategies". This challenge arises from the heterogeneity of government entities, which hinders seamless interoperability and secure data exchange. To overcome such challenges, Semantic Web technologies - such as RDF, OWL, and SPARQL - have been increasingly adopted to construct unified, standards-based knowledge frameworks. These technologies support semantic interoperability across distributed systems and offer promising tools for integrating government services. However, as noted in [2], "much research in the Semantic Web and Linked Data domain has focused on enabling the sharing of open datasets" often overlooking essential security and access control requirements that are critical in sensitive domains such as public administration. This research focuses on a critical aspect of secure e-government: access control. Although ensuring robust security in public administration is imperative, the integration of semantic web methods into these systems frequently exposes vulnerabilities—particularly within access control mechanisms. In response, we propose an innovative solution that reinforces the conventional Role-Based Access Control (RBAC) model. Our approach integrates ontology-driven methodologies to dynamically implement access policies, ensuring that only authorized users gain access to sensitive information. The central hypothesis of this study is that embedding semantic web technologies into access control frameworks not only improves data interoperability but also significantly enhances security by preventing unauthorized access and ensuring proper user authentication. To validate this hypothesis, we designed and implemented a prototype using Apache Jena Fuseki alongside semantic web technologies such as RDF, OWL, and SPARQL. The prototype was evaluated in an e-government context, demonstrating that dynamic semantic reasoning and flexible policy updates can effectively meet the complex security requirements of distributed public services. The results indicate that our approach supports scalable, interoperable, and secure e-government systems, paving the way for broader adoption of semantic web technologies in public administration. This paper contributes to bridging the gap between theoretical research and practical application in the fields of information security, semantic web, and public administration. By integrating semantic reasoning with enhanced access control, our work presents a practical framework that addresses the key challenges of data interoperability and security within e-government systems. A review of the literature reveals extensive research on both Semantic Web applications and e-govern-

ment systems. Previous studies have tackled issues such as data heterogeneity, interoperability challenges, and security vulnerabilities. Multiple methodologies have been proposed for integrating semantic technologies into public administration, with particular attention to the dynamic enforcement of access control policies and the use of ontologies for modeling complex governmental data. Building on these findings, our work presents a comprehensive solution that unifies semantic data sharing with enhanced access control, thereby addressing both integration and security requirements in e-government environments.

Semantic Web-Based E-Government

Semantic Web technologies have become a cornerstone for achieving interoperability and data integration in e-government systems. Study [3] mapped a range of case studies; for example, [4] developed a domain ontology for Nepal's citizenship certificates, improving issuance accuracy and efficiency, and [5] introduced semantically reusable Web Components that measurably enhance response time and interoperability—while also noting that practical deployment details remain underexplored. Concrete prototypes further illustrate these insights: [6] harmonized civil, health, and education schemas into a unified OWL ontology, enhancing consistency and query precision; and [7] implemented an OWL-based integration platform in Kuwait, enabling real-time semantic queries across ministries. At the national level, [8] showcases Finland's Semantic Web infrastructure: a cross-domain ontology "layer cake" and a series of Linked Open Data portals built on SPARQL endpoints. For over two decades, this infrastructure has supported hundreds of applications, proving that scalable, government-wide semantic integration is both feasible and impactful. Study [9] surveyed RDF, OWL, and SPARQL applications across public-sector services, categorizing technical and socio-economic challenges—particularly around security and real-world deployment—and concluded that the semantic web lacks the maturity of a production-grade artifact, calling for increased focus from both academia and industry. Together, these studies trace the evolution from targeted domain ontologies to large-scale national frameworks, paving the way for our ontology-based RBAC solution that combines semantic data sharing with dynamic access control.

Semantic Web-Based Access Control

Since the inception of semantic web technologies, many studies have investigated their application in access control to address security vulnerabilities in distributed systems. Researchers have explored various models, including DAC (Discretionary Access Control), MAC (Mandatory Access Control), RBAC,

and ABAC (Attribute-based Access Control). These studies have often yielded the following findings:

- For MAC and DAC, studies such as [10] have focused on defining vocabularies that support multiple access control models using DAML+OIL (Darpa Agent Markup Language + Ontology Inference Layer) ontologies. Similarly, [11] proposed an attribute-based model to overcome heterogeneity in distributed environments, supporting MAC, DAC, and RBAC.
- In the domain of RBAC, recent works have advanced semantic role modeling and multi-domain integration. [12] proposes an intelligent RBAC framework that defines “semantic business roles” via OWL ontologies and enables policy evaluation across organizational boundaries. Additionally, [13] introduced a semantic security platform that implements an enhanced RBAC model (merging RBAC and ABAC) using ontology modeling techniques. [14] presents a feature-oriented survey of ontology- and rule-based access control systems with a focus on conflict resolution and dynamic decision making. [15] demonstrates an ontology-based data access case study in which semantic queries enforce role assignments and permissions within a distributed environment, validating practical applicability.
- Regarding ABAC, studies have focused on attribute-driven policy enforcement and fine-grained control. [16] introduces a semantic ABAC model based on ontology-defined attributes and context rules for adaptive access decisions. [17] extends semantic ABAC to e-Health, designing an ontology that maps user, resource, and contextual attributes to enable secure, fine-grained medical data access, and [18] presents a general ontology for access control that performs effectively in large-scale, heterogeneous environments. Collectively, these studies demonstrate that semantic web technologies can effectively support various access control models. However, challenges remain when applying these technologies in environments with sensitive data, such as e-government systems

MATERIALS AND METHODS

In this section, we propose a solution for information sharing in an e-government environment, as well as an access control mechanism within that environment. Our approach builds on foundational ontology-design methodologies from recent research studies [19, 20, 21], adheres to widely accepted semantic web standards, including RDF, RDFS (Resource Description Framework Schema), OWL, and SPARQL, and employs Protégé platform and GraphDB’s visual graph feature for ontology development and visualization. Semantic data is stored, queried, and man-

aged in an Apache Jena Fuseki triple store, while the Semidesk Trinity framework provides seamless .NET integration with Fuseki. The web application layer is implemented using ASP.NET MVC5 and ASP.NET Core within Visual Studio 2022. This foundation enables the implementation of a scalable, interoperable, and secure e-government system that integrates semantic reasoning and dynamic access control policies.

Proposed Solution for E-Government Information Sharing

In this study, we assume the existence of four government entities, each developing its own application while enabling information and knowledge sharing among themselves. These entities are:

*Ministry of Health *Ministry of Labor
 *Ministry of Higher Education *Civil Registry

To facilitate interoperability, a simplified yet expandable ontology was designed for each entity.

- **Ministry of Health Ontology:** This ontology consists of the following classes: mc-Patient, mc-Hospital, mc-Injury, and mc-InjuryDetails. See Figure 1.

- **Ministry of Labor Ontology:** This ontology includes the classes: mc-Beneficiary, mc-EmploymentRequest, and mc-FamilySupport.

- **Ministry of Higher Education Ontology:** This ontology is composed of the classes: mc-StudentProfile, mc-Course, and mc-Exam.

- **Civil Registry Ontology:** It contains a single core class: mc-PersonProfile, which stores the personal information of citizens. And an auxiliary class mc-Citizen is introduced as a container to link the other ontologies. See Figure 2. The ontology model ensures that each government entity maintains its own structured data while remaining interoperable through shared concepts.

Information Sharing Among E-Government Ontologies

The proposed solution establishes semantic relationships between different government entities by defining mc-Patient (Ministry of Health), mc-Beneficiary (Ministry of Labor), and mc-StudentProfile (Ministry of Higher Education) as subclasses of mc-PersonProfile class (Civil Registry). See Figure 3. By applying inheritance principles, any instance created in the sub-classes automatically inherits its personal data from the corresponding mc-PersonProfile instance in the Civil Registry. This ensures that all citizens—whether they are students, beneficiaries, or patients—are first recognized as individuals within the national Civil Registry system before being associated with specific government sectors. This ontology-driven approach enhances data consistency, reduces redundancy, and enables seamless information retrieval across multiple govern-

ment institutions, forming the foundation for a unified and interoperable e-government system. To demonstrate information sharing among e-government ontologies, several SPARQL query examples are provided in the supplementary materials.

Proposed Solution for Access Control

The RBAC (Role-Based Access Control) model was selected as the foundation of the proposed solution due to the structured role-based nature of e-government institutions. Since government environments typically have well-defined actor roles, RBAC provides a policy-neutral, manageable, and scalable approach to access control. As stated in study [22]: “Role-Based Access Control models appear to be the most attractive solution for providing security features in multidomain e-government

infrastructure. RBAC features such as policy neutrality, principle of least privilege, and ease of management make them especially suitable candidates for ensuring safety in e-government environment”. RBAC is commonly classified into four levels, ranging from the simplest to the most advanced: Flat RBAC, Hierarchical RBAC, Constrained RBAC, Symmetric RBAC. Each level builds upon the previous one. Since the goal of this research is to develop a simple yet expandable solution, the proposed approach implements Flat RBAC, while ensuring that future extensions to Hierarchical and Constrained RBAC are feasible. Following ontology design principles, we begin by modeling a core RBAC ontology, depicted in Figure 4, that conforms to the Flat RBAC standard



Figure 1 .Ministry of Health Proposed Ontology

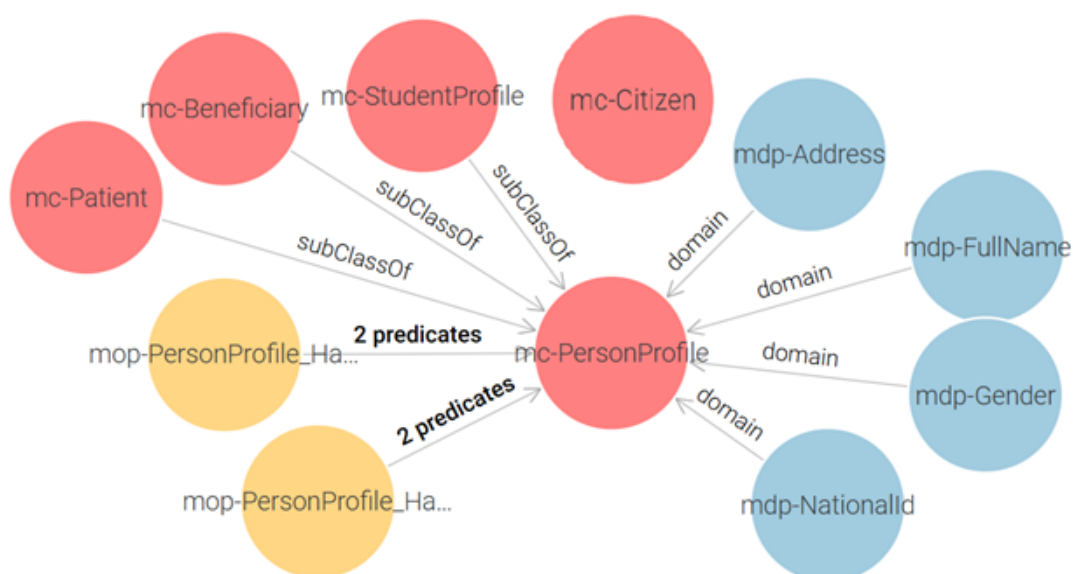


Figure 2. Civil Registry Proposed Ontology



in real-world applications due to its abstract handling of permission granularity and lack of support for multi-application contexts. To address these limitations and enable the application of RBAC in real deployment environments, we extend and restructure the initial model into a more implementation-oriented ontology, as shown in Figure 5.



This model replaces the triplet of Permission, Action, and Resource with a single Method class, which represents functions or procedures within the system that users interact with. It also adds two more classes: Credential (for user authentication), and Application (for managing access within multiple systems). This ontology enables administrators to assign methods (i.e., grouped action-resource operations) to roles per application, and to authenticate users via credentials before role activation. The proposed model successfully meets the fundamental requirements of the Flat RBAC standard:

1. Users acquire permissions (Methods in our case) through roles.
2. Both user-role assignments and permission-role assignments (Method-Role assignments in our case) follow a many-to-many relationship.
3. The system supports user-role review.
4. Users can exercise permissions associated with multiple roles simultaneously.

These compliance criteria were verified through SPARQL queries, which are provided in the supplementary materials for reference.

RESULTS

The research resulted in the development of the following applications:

1. Access Control Application:
 - This application enables administrators to define users, roles, and permissions, effectively implementing the Role-Based Access Control (RBAC) model.
 - Additionally, it provides an API service that allows e-government applications to request user access verification and make allow/deny decisions accordingly.
2. E-Government Applications:
 - These applications utilize the access control system for managing secure access while supporting interoperable data exchange among government entities.

Implementation of the Access Control Management Web Application

A web-based application was developed to serve as the administrative interface for the Access Control System. This application was built using ASP.NET MVC5, leveraging the Semiodesk Trinity platform for data layer integration. It provides system administrators with full control over Applications, Users, Roles and Permissions (Methods). Additionally, the system is designed to manage

itself, incorporating authentication and authorization mechanisms.

Authentication and Authorization Process

1- User Login (Authentication):

- The system verifies user credentials by searching for a matching username and password in the stored user data.
- Upon successful authentication, the system retrieves the roles assigned to the user and the permissions linked to those roles.

2- Authorization Mechanism:

- Once authenticated, the system determines whether the user is authorized to access a specific method.
- For example, when a user requests the home page (Index) within the HomeController of the Access Control Application, the system evaluates whether the method's signature (AppRbac_Home_Index) exists within the user's assigned permissions.
- If a match is found, the user is granted access, and the requested page is displayed.

This authorization mechanism is enforced throughout the application. Each time a user navigates between interfaces or performs an action, the system validates their authorization to invoke the corresponding method, ensuring role-based access control. The following Figure 6 illustrates one of the user interfaces of the application. Integration with E-Government Applications via AppMgr.Api

A dedicated API service (AppMgr.Api) was developed to facilitate communication between the Access Control System and e-government applications. This service is invoked by e-government applications whenever a user attempts to log in.

1. When an e-government application sends a login request, it includes the username and password of the user.
2. The authentication process follows the same mechanism described earlier:
 - The system verifies the credentials.
 - If authentication is successful, the user's roles and permissions are retrieved.
3. The API response includes:
 - The user's assigned roles and permissions.

- The URL to which the user should be redirected upon successful login.
4. Unlike the Access Control Management Web Application, authorization is not handled by the API itself. Instead, each e-government application processes authorization

internally, relying on the permissions received from the API.

This modular approach ensures flexibility, allowing each e-government system to enforce role-based access control (RBAC) policies based on its specific operational requirements. **E-Government Applications and Information Sharing Between them**

اسم الدور	اسم الدور بالعربي	مدير نظام؟	معرفة التطبيق
RBAC Admin	مدير نظام ضبط الوصول	نعم	تطبيق ضبط الوصول
MOLrole2	دور موظف وزارة العمل 2	لا	تطبيق وزارة الشؤون الاجتماعية والعمل
MOLrole	دور موظف وزارة العمل	لا	تطبيق وزارة الشؤون الاجتماعية والعمل
MOHrole2	دور موظف وزارة الصحة 2	لا	تطبيق وزارة الصحة
MOHrole	دور موظف وزارة الصحة	لا	تطبيق وزارة الصحة
MOHErole2	دور موظف وزارة التعليم العالي 2	لا	تطبيق وزارة التعليم العالي
MOHErole	دور موظف وزارة التعليم العالي	لا	تطبيق وزارة التعليم العالي
MOCrole2	دور موظف السجل المدني 2	لا	تطبيق السجل المدني

Figure 6. Roles Management in Access Control Application

تسجيل الخروج

المرضى أنواع الاصابات المستشفيات

إضافة مريض

الرقم الوطني
22345

الاستعلام حسب الرقم الوطني

الجنس
أنثى

العنوان
حمص

الاسم الكامل
Rama Example

إضافة

[العودة لقائمة المرضى](#)

© 2025 - تطبيق وزارة الصحة

Figure 7.(Add Patient) Interface in the Ministry of Health Application

The e-government applications were developed using ASP.NET Core, in combination with Semiodesk Trinity and the Apache Jena Fuseki triple store. These applications were integrated with the Access Control Service, which manages both authentication and authorization processes.

1. Example: Patient Registration in the Ministry of Health Application

- As shown in Figure 7, when registering a new patient in the Ministry of Health application, the system first performs a query using the citizen's national ID in the Civil Registry application.
- The registry retrieves and returns personal information, and the Ministry of Health user adds the patient's medical details.

2. Similarly, new beneficiary registrations in the Ministry of Labor application and student registrations in the Ministry of Higher Education application rely on retrieving personal details from the Civil Registry. This demonstrates the seamless interoperability and efficient data sharing enabled by the semantic integration model.

3. Example: Sharing Medical Records Between Applications

- Figure 8 illustrates the family support interface in the Ministry of Labor application, where the amount of support is calculated based on the injury

percentage of each beneficiary.

- The injury percentages data originates from the Ministry of Health ontology, further validating the effectiveness of semantic information sharing across government applications.

Reasoning Activation in E-Government Applications

To enhance data inference capabilities, a reasoning engine was activated within the Fuseki triple store using the OWLMicroFBRuleReasoner. Example of Automated Inference:

- The reasoning engine allows the system to derive new knowledge that was

الاسم الكامل	نسبة التعويض الصحي	أساس التعويض	المجموع
Mhd Example	35 %	100000	135000
Mazen Example	10 %	150000	165000

© 2025 - تطبيق وزارة الشؤون الاجتماعية والعمل

Figure 8. (Family Support) Interface in the Ministry of Labor Application

not explicitly stored in the triple store.

2- Consider the following inverse relationships between the Exam and Course classes:

- Exam \rightarrow has_exam \rightarrow Course
- Course \rightarrow exam_has_course \rightarrow Exam

3- If the triple (course1 has_exam exam1) is added, the reasoning engine automatically infers the inverse relationship:

- (exam1 exam_has_course course1)

4- This inference is dynamically added to the e-government dataset, ensuring data consistency and completeness.

5- The effectiveness of this semantic reasoning mechanism was successfully tested in the student exam details interface, along with several other logical inferences within the applications.

DISCUSSION

Our work advances both semantic information sharing and access control in ways that address the limitations noted in prior studies. Unlike study [7], which proposed ontologies without implementation, we developed a working prototype that demonstrates real-time data exchange across government

domains. In contrast to study [1], which lacked a mechanism to identify the appropriate authority for a given service, our model integrates an ontology-driven RBAC system to securely handle such decisions. From an access control perspective, the study validates that Semantic Web technologies can effectively implement a Role-Based Access Control (RBAC) model through ontology-driven mechanisms. While most access control research remains theoretical or limited to less-sensitive domains such as Online Social Networks or cloud platforms [18], our solution is applied in an e-government context, managing sensitive data through a fully implemented, policy-aware system. While this work focused on the Flat RBAC model, its semantic foundation facilitates natural extensions to Hierarchical and Constrained RBAC. Evaluation Criteria and System Assessment To further assess the quality and applicability of the proposed system, we evaluated it against commonly accepted criteria in semantic e-government research, as outlined below: This qualitative evaluation demonstrates that the proposed solution is not only conceptually sound but also practical, modular, and aligned

with real-world public-sector requirements.

CONCLUSIONS AND RECOMMENDATIONS

This research introduced a semantic web-based framework for secure information sharing and access control in e-government environments. The study confirmed that by leveraging ontologies and reasoning engines, government systems can achieve improved interoperability, reduced redundancy, and scalable architecture—while also supporting dynamic, fine-grained access control mechanisms. The integration of ontology modeling with access control policies strengthens both security and flexibility in distributed digital services. Based

on these findings, the following recommendations are proposed:

- Expand e-government ontologies by integrating additional domain-specific concepts and linking to existing public ontologies on the web to enhance service coverage.
- Extend the access control ontology to support Hierarchical RBAC and Constrained RBAC, leveraging OWL constructs to model complex permission structures.
- Deploy the developed applications on the public web, hosted by trusted national IT infrastructures, to enable citizen-facing services while maintaining data protection and system integrity.

Table 1 - Qualitative Assessment of the Proposed System Based on Semantic E-Government Evaluation Criteria	
Criterion	Assessment in Proposed Solution
Interoperability	The solution enables seamless integration of data from diverse government domains through a shared Civil Registry ontology. This eliminates the need for direct APIs between systems and supports federated SPARQL queries.
Scalability	The ontology design uses subclassing (e.g., mc-PersonProfile) to allow future extensions with minimal changes. New entities can be introduced without structural redesign.
Logical Consistency	The use of inherited properties ensures that all individuals (students, patients, etc.) remain logically tied to their base identity, reducing data duplication and inconsistency.
Semantic Reasoning	The ontology structure enables automated inference (e.g., if a citizen is a beneficiary, the system infers they are also a person), improving query completeness and accuracy.
Access Control	The RBAC ontology enforces user-role-method relationships through a fully implemented access control service, validated via SPARQL queries. The model supports user-role reviews and many-to-many role-method mappings.
Reusability	The modular ontology structure and application-oriented design allow the solution to be adapted across different technical environments (semantic or conventional).

REFERENCES

1. Lamharhar H. A Semantic modelling approach for e-government domain. 2016; 10.13140/RG.2.1.4858.1209.

2. Krrane S, Villata S, d'Aquin M. Privacy, security and policies: A review of problems and solutions with semantic web technologies. Semantic Web. 2018 Jan 24;9(2):153-61.

3. Altahir BH, Karrar AE, Mohammed SS. The Impact of Semantic Web and Ontology to Improve E-government Services: A Systematic Review. Indonesian Journal of Electrical Engineering and Informatics (IJEI). 2023 Dec 26;11(4):1082-96.

4. Bastola R, Campus P. Developing domain ontology for issuing certificate of citizenship of Nepal. Journal of Information Technology. 2020 May 16;2(02):73-90.

5. Žitnik S, Pipan KK, Jesenko M, Lavbič D. Semantic reusable Web Components: A Use case in e-government interoperability. Uporabna informatika. 2022 Oct 17;30(4).

6. Tshering Y. Ontology-based approach of e-government for interoperability. Int J Res Appl Sci Eng Technol. 2021;9:3197-202.

7. Alshehab AB, Alazemi NN, Alhakem HA. Semantic integration sharing for e-government domains ontology: Design and implementation using owl. Journal of Theoretical and Applied Information Technology. 2019 Mar 31;97(6):1820-31.

8. Hyvönen E. How to create and use a national cross-domain ontology and data infrastructure on the Semantic Web. Semantic Web. 2024 Oct 4;15(4):1499-513.

9. ALSHEHAB' AB, Alazemi N, Yousef M, Alfayly A. Challenges of applying semantic web approaches on e-government web services: Survey. International Journal. 2021 Mar;10(2).

10. Kodali N, Farkas C, Wijesekera D. An authorization model for multimedia digital libraries. International Journal on Digital Libraries. 2004 Nov;4:139-55.

11. Yague MI, Mana A, Lopez J, Troya JM. Applying the semantic web layers to access control. In14th International Workshop on Database and Expert Systems Applications, 2003. Proceedings. 2003 Sep 1 (pp. 622-626). IEEE.

12. Ghazal R, Malik AK, Qadeer N, Raza B, Shahid AR, Alquhayz H. Intelligent role-based access control model and framework using semantic business roles in multi-domain environments. IEEE Access. 2020 Jan 9;8:12253-67.

13. Hosseinzadeh S, Virtanen S, Díaz-Rodríguez N, Lilius J. A semantic security framework and context-aware role-based access control ontology for smart spaces. InProceedings of the International Workshop on Semantic Big Data 2016 Jun 26 (pp. 1-6).

14. Gicquel PY, Bouché-Pillon J, Zaraté P, Aussenac-Gilles N, Chevalier Y. Ontologies and rules for access control: a feature oriented survey. In1st Workshop on Collaboration in knowledge discovery and decision making: Applications to sustainable agriculture (DECISIONING 2022) 2022 Jun 30 (pp. 1-12).

15. Can Ö, Ünalır M. Ontology Based Access Control: A Case Study through Ontology Based Data Access. Dokuz Eylül Üniversitesi Mühendislik Fakültesi Fen ve Mühendislik Dergisi. 2023;25(74):417-32.

16. Bayram U. Semantic-Attribute Based Access Control (Master's thesis).2020.

17. Arshad H. Toward Semantic Attribute-Based Access Control Fine-grained protection of data in e-Health. 2022

18. Imran-Daud M, Sánchez D, Viejo A. Ontology-based access control management: Two use cases. InInternational Conference on Agents and Artificial Intelligence 2016 Feb 24 (Vol. 2, pp. 244-249). SciTePress.

19. Noy N, McGuinness D. Ontology development 101: a guide to creating your first ontology. Stanford (CA): Knowledge Systems Laboratory, Stanford University; 2001. 32.

20. Ben Mahria B, Chaker I, Zahi A. A novel approach for learning ontology from relational database: from the construction to the evaluation. Journal of Big Data. 2021 Jan 28;8(1):25.

21. Haw SC, May JW, Subramaniam S. Mapping relational databases to ontol-



ogy representation: A review. In Proceedings of the 1st International Conference on Digital Technology in Education 2017 Aug 6 (pp. 54-58).

22. Milić P, Kuk K, Civelek T, Popović B, Kartunov S. The importance of secure access to e-government services. *Communications*. 2016;26(16):1873-893.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to Hani Mohammad for his invaluable technical support throughout the development of the applications, and for his continued encouragement. Special thanks to Sebastian Faubel, Co-Founder of Semiodesk, for his valuable guidance and generous support during the implementation phase.

Fund: No fund.

Author Contributions: Conceptualization & Methodology:

Sary Jouhara - Investigation: Sary Jouhara - Project admin-

istration: Sary Jouhara - Supervision: DR. Mohamad Aljnidi

- Writing – original draft: Sary Jouhara - Writing – review & editing: Sary Jouhara

Competing Interests: Authors declare that they have no competing interests

Data and Materials Availability: All implementation-related ontologies used in this study are publicly available at:

<https://github.com/sajo-work-it/semantic-egov-RBAC>

Supplementary Materials: All data are available in the main text or the supplementary materials.