applied sciences

MDPI

Article

Built Environment Cybersecurity: Development and Validation of a Semantically Defined Access Management Framework on a University Case Study

Kaznah Alshammari [1,*], Thomas Beach [2], Yacine Rezgui [2] and Raed Alelwani [3]

[1] Department of Information Technology, Faculty of Computing and Information Technology, Northern Border University, Rafha 91911, Saudi Arabia
[2] School of Engineering, Cardiff University, Cardiff CF24 3AA, UK; beachth@cardiff.ac.uk (T.B.); rezguiy@cardi.ac.uk (Y.R.)
[3] Department of Architectural Engineering, Faculty of Engineering, Al-Baha University, Al Aqiq 65527, Saudi Arabia; rsalelwani@bu.edu.sa
* Correspondence: khaznah.alshammari2@nbu.edu.sa

Abstract: To achieve the potential of smart cities, there is a strong requirement to use a set of useful, but still accessible services within smart city systems. Interoperability challenges and roadblocks for software developers and integrators are well-known consequences of fragmented semantics across different contexts. Furthermore, in the smart city context, there is a need to ensure the security and identity of real-world services operating on this data through the adoption of access control principles (authorization and authentication). The use of ontologies to unify the diverse semantics of multiple domains is one strategy that has had considerable success in the past. This paper describes an access management ontology in smart cities developed to enable the interoperability of physical built environment assets, sensing and actuation devices and current built environment services with existing security standards, digital twin and Building Information Model (BIM) datasets. It also provides interoperability between user interfaces and the actors who use them in the context of establishing an access management in smart cities framework for the built environment. This has been validated through its implementation in the Cardiff Urban Sustainability Platform (CUSP), deployed to manage a variety of smart services on a university campus. This validation has successfully shown the ability of the ontology to function as intended in the context of a digital twin, thereby offering single sign-on and suitable access control.

Keywords: access management; cybersecurity; NeOn; ontology; semantic

Citation: Alshammari, K.; Beach, T.; Rezgui, Y.; Alelwani, R. Built Environment Cybersecurity: Development and Validation of a Semantically Defined Access Management Framework on a University Case Study. *Appl. Sci.* **2023**, *13*, 7518. https://doi.org/10.3390/app13137518

Academic Editor: Luis Javier García Villalba

Received: 15 May 2023
Revised: 18 June 2023
Accepted: 19 June 2023
Published: 26 June 2023

1. Introduction

A smart city anchored by a cyber physical system can provide an intelligent solution capable of enhancing how urban services such as weather, energy and transport perform by combining data from the Internet of Things (IoT), building information modelling (BIM) and data mined from Internet sources and directly from inhabitants. These ingenious methods will significantly improve the efficiency of a city's operations. Although such improvements are expected to significantly improve infrastructure in the built environment, they frequently present technological obstacles that must be addressed. Indeed, the variety of data sources and knowledge modelling may limit the capacity for decision-making [1,2]. There is also the important problem of defending against cyberattacks and appropriately enforcing access controls [3]. Integrating access management in smart cities in digital twins so that it can be applied in the built environment has proven to be a difficult task to date.To preserve the safety and identity of their physical twin, digital twins must be safe. Methodologies and data models are required to ensure effective protection across platforms, domains and scales [4,5]. Access management approaches ensure that only relevant

users who are correctly identified can access and utilize resources [6,7]. Cyber-physical systems and IoT devices must be integrated with BIM datasets, digital twins, existing built environment services, current security standards, as well as newly developed user interfaces and the actors who use them. There have already been implementations in each of these fields, each with its own semantics, data structures and application programming interfaces (APIs). Therefore, in a bid to bring together such diverse attempts to produce a unified means of access management, this paper sets out to formalise the associated concepts, aligning them with the prevailing ontologies and concepts by means of semantic modelling. The aim of this paper is to answer the following research question: Can a semantically defined access management framework in smart cities prove suitable to manage the security of smart services deployed in the built environment? To answer this question, this paper follows a semantic approach, specifying and subsequently validating an access management framework in smart cities that is underpinned by formalized semantics. This access management framework in smart cities is built upon [8] validating this work through a set of use cases in a university context. This semantic approach is critical given the framework's intersection with prevailing built environment services, cyber-physical systems, IoT devices, physical built environment assets, digital twin and BIM datasets [9]. Thus, the current paper utilizes a rigorous ontology specification approach to formalize this framework. The remainder of this paper presents a background and related work of urban cities applications and cybersecurity functions; the methodology of a semantically specified access management framework in smart cities; defines the access management framework in smart cities; and presents ontology access management framework in smart cities development. The paper then develops and validates an access management ontology for built environment cyber-physical systems and inferences.

2. Background and Related Work

The construction industry is currently working to build smarter buildings and cities [8]. To create and distribute information, it relies on ongoing improvements in information and information communication technology (ICT). Recent technological advancements have resulted in advancements in mobile communications, always-on connectivity, faster communication speeds and less expensive sensors [8]. Not only has technology been more prevalent, but there has also been a greater integration of cyber systems and physical infrastructure [9], also known as the IoT. The increasing adoption of this technology, for example, has been fueled by falling costs and breakthroughs in communication networks [10,11]. As a result, there are countless chances for information of the built environment to be extremely valuable [3]. BIM is an example of a built-environment information model that has emerged as a new stage in the expanded digitization of built-environment data in the expanded digitization of built-environment data in the architecture [12], engineering [13], construction [14] and facilities management (AECFM) business [4]. In this changing context, BIM can be utilized in a layered model to assist visualize and categorize the various elements, with a focus on how to best enable knowledge and ICT to enhance business services [15]. This entails the employment of a sensing layer, a mode of communication and capabilities for processing, storing and analyzing data [9]. The application, business, innovation and governance layers are provided on top of this. Sensor networks had previously focused mainly on providing communication infrastructure for cyber–physical systems (CPSs) [9]. As a result, the growing notion of digital twins provides CPSs with a new possible outcome in terms of monitoring, modeling, optimizing and predicting the status of built environment assets [16,17]. Cybersecurity is a major worry for everyone who uses CPS or digital twins [3]. Cybersecurity is the function of securing access to devices and services as well as preventing unauthorized access to data stored on these devices, which drives CPS services [3]. Companies employed in the built environment must include cybersecurity into their policy, architecture and operations [18]. All sides are concerned about being willing to confront cybersecurity challenges in a positive way. Furthermore, to maximize the efficiency of the overall output value, cybersecurity plans should be properly

linked with organizational and information technology (IT) strategies [19]. Within the build environment, especially in terms of smart cities and cyber–physical systems, it is becoming recognized that existing security approaches are not fit for purpose [9]. Future research goals in this area have been defined as a result [9]:

(1) Extend BIM specifications to satisfy IoT requirements.
(2) Improve BIM standards so as to promote the provision of effective cybersecurity.
(3) Ensure that effective support for cybersecurity and the IoT is incorporated into digital twin and future city standards.
(4) Thoroughly combine cybersecurity concepts with the prevailing built environment data standards.

In response to this, this paper will tackle the following two recommendations. To ensure that standards for future cities and digital twins can incorporate IoT and cybersecurity concerns, an access management framework in smart cities will be created. Furthermore, this work will be built as an ontology for it to be combined with present as well as future cybersecurity concepts. To achieve this, the current paper aims to elicit the requirements of the access by investigating the empirical literature and proposing recommendations regarding how access management should be adopted in the built environment. This involves conducting reviews of the latest technological innovations relating to access management, smart cities, digital twins, the IoT and BIM, in addition to gauging the opinions of industry with regards to access management in the built environment and the challenges that must be overcome before further progress can be made.

3. Methodology

This section describes the paper's methodology. As described in Section 1, the research question being answered in this paper is as follows: Can a semantically defined access management framework in smart cities prove suitable to manage the security of smart services deployed in the built environment?

Answering this question is important because whether an access management framework can secure data from digital twins is crucial to the possible creation of secure built environment solutions across a wide range of use cases in smart cities, such as healthcare, education and weather environments.

This research question will be answered through the following steps:

(1) Define the concept of an access management framework for the built environment. It is our view that semantics must be utilised here to provide the formalised management of access management concepts for the built environment which can then, in turn, enable the wide range of tools and standards utilised in the built environment to be applied in an interoperable manner, thereby making it possible to make use of the defines access management concepts (see Section 4).
(2) Eliciting the formal specification of the framework using the NeOn methodology (Section 5).
(3) Development of the semantic access management framework in smart cities using both new and existing ontological resources (Section 5.2).
(4) Validation of the framework whereby the ontology is applied in a use case via the CUSP platform [2]. This entailed the integration of the ontology and access management framework on the available platform so that a range of case studies could be applied to validate the framework. The results confirmed the ability of the ontology to function as intended in a digital twin setting, offering single sign-on and suitable access control [20] (see Section 6). The decision was taken to apply the NeOn approach for the second step owing to the fact that the supporting documentation was available, it offered a scenario-based approach and because of the available knowledge [21]. Consequently, digital twin access management for a built environment ontology was achieved using the NeOn approach [21,22]. More specifically, this entails the application of a four-phases process:

Phase 1 (Initiation): The initial phase specifies the ontological requirements, drawing upon insight gleaned from analysing case studies relating to the built environment (see Section 5), the findings of the survey [23] and a review of the empirical literature [9].
Phase 2 (Re-use phase): The second phase involves analysing the available ontological resources to establish the ways in which they can be redeployed in the ontology that is devised. As part of this process, the semantic resources currently available in the access management and built environment domains will be factored in (see Section 5.2). In addition, there is an assessment of the resources that are non-ontological, enabling them to be formalised and re-engineered in a way that brings them into line with the ontological resources that are already in place. This second phase was undertaken for both case studies utilised to establish the requirements Section 5.3). The main purpose of this investigation is to establish the concepts and terminologies which will contribute to the ontology.
Phase 3 (Design): The third phase involves developing the final ontology with reference to the specified requirements as well as the re-engineering of the non-ontological and ontological resources (described in Section 6).
Phase 4 (Implementation): The developed ontology will be implemented and validated on a digital twin case study within the university buildings (described in Section 6.2).

4. Semantically Defined Access Management Framework in Smart Cities

The development of an access management framework is essential because previous work has identified the key requirement for security in smart cities as follows: it must be able to integrate and align across multiple domains, including built assets, existing digital services as well as actors themselves. These requirements align with the advantages provided by a semantic approach. As such, it has been possible to propose an access management framework that is semantically defined [23]. When it is necessary for the formal relationships established between the built environment and access management concepts to be modelled, it is recommended that the ontology and semantic modelling concepts are utilised. This entire approach is required since interoperability is a critical component of achieving holistic and accessible services in a smart city. Common problems include existing fragmented semantics across differing contexts that cause interoperability issues and create obstacles for software developers and integrators.

Figure 1 provides an illustration of the process by which the core aspects of semantics required to facilitate digital twin access management are identified by the semantically defined cybersecurity framework, as well as how these disparate elements are combined to produce a unified semantic model.

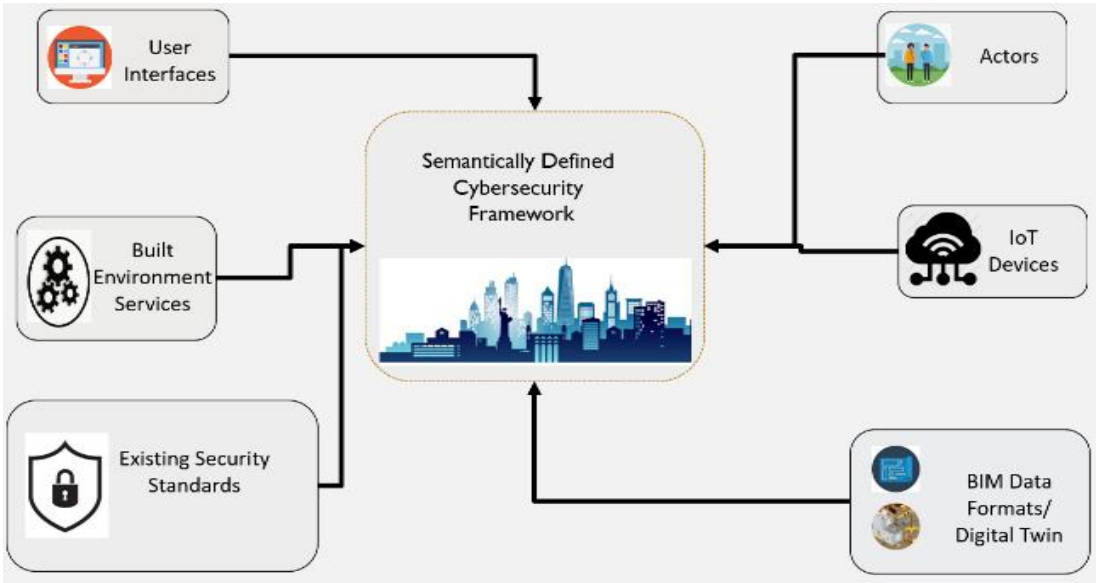

Figure 1. Semantically defined access management framework in smart cities.

Thus, the justification for the creation of the framework will utilise semantic Web technologies to combine cyber security standards currently applied in various domains to model the physical items that comprise cities including processes, individuals and structures, as well as the digital services operating on them. Following the definition of the concept of the access management framework in smart cities, this section provides a definition of the access management ontology's specification which will deliver it for smart cities. The access management ontology for the built environment will be developed using the NeOn approach [24]. The initial process when applying the NeOn approach is the ontology requirement specification (ORS) [24]. This is required to determine the limits for the domain semantic modelling and emphasises the need to have access to suitable information. More specifically, it entails establishing the overarching aim of the ontology under development, the uses to which the ontology can be deployed, and the standards which need to be satisfied by the ontology [20]. The primary aim of the ontology is to identify the integrations that the access management framework requires with regards to formalised semantics. This provides integration with regards to innovative user interfaces, BIM datasets, digital twins, prevailing security standards, the available built environment services, cyber-physical systems, IoT devices, and physical built environment assets (see Figure 2). Therefore, digital twins will have an access management framework that feature formalised semantics to enable single sign-on (SSO) throughout all services relating to the built environment, ensure that all data remains secure and confidential, and apply access control. This is supported by digital twins' access management specifications. The last step involves identifying the criteria the ontology is required to satisfy. Applying the NeOn approach, this entails providing definitions for the competency questions. These questions help to determine how complex an ontology is by listing questions which should be capable of being answered using knowledge that is ontology-based [20,24–26].

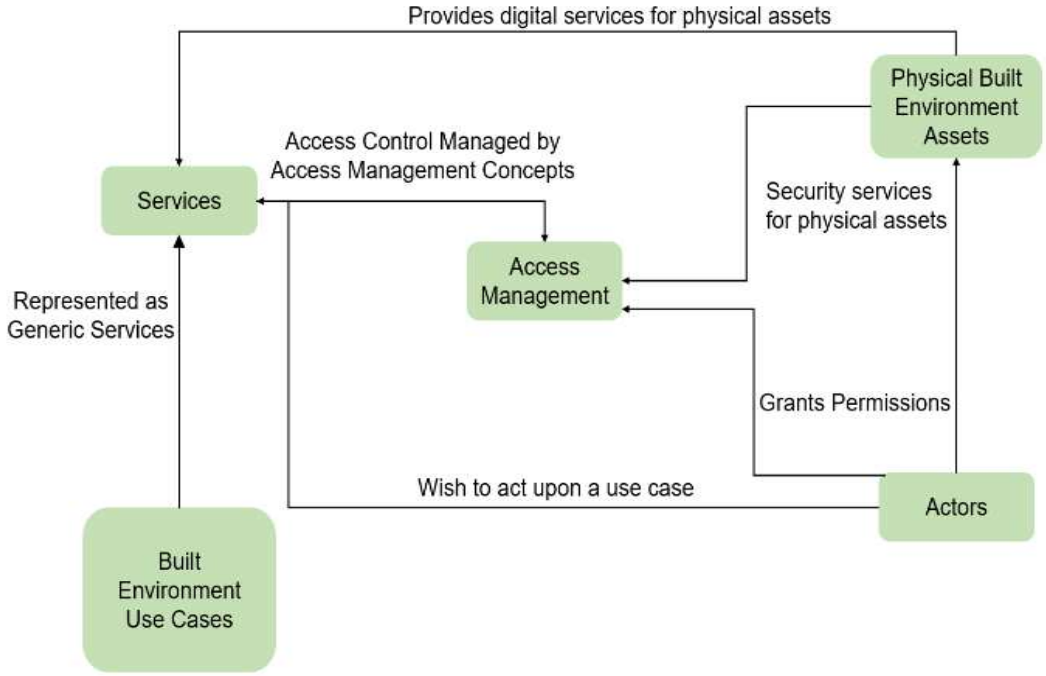

Figure 2. Access management framework in smart cities.

Five categories of competency questions were compiled (security standards, built environment services, actors, built environment data format, IoT devices) that reflect the aspects of access management being integrated by the model: objects, actions and individuals and the impact they have in terms of the efficiency of security efforts. The following sections discuss how the access management ontology of smart cities can be developed.

5. Ontology Access Management Framework Development

It is necessary to formally specify the key elements of the framework by applying an ontological modelling approach that is representative of domain information and saves time and money during the development and operation stage... In the development stage, the formal definition of semantics for access management defined makes the specification, development and integration of software tools that require access management easier and more strong. Furthermore, at operation time, it enables easier management of access management configuration and setting dynamically across an assets life cycle [27]. This section will address the analysis of existing ontological resources, re-engineering of built environment non-ontological resources and a built-environment case study. These include a use case of a smart parking system and an attendance management system. These were selected to represent an infrastructure and a building-based use case. End-users (students, members of staff) using the smart parking system are given access to a personalized mobile application (parking application). They can use this app to find available parking spots at a university, get directions to the desired spot, reserve a space, check the amount of time they have left to park and get notified when that time is up. First, the user is required to connect to the app through their mobile telephone [28].

5.1. Re-Engineering of Built Environment Non-Ontological Resources

An ontology is, by definition, a formal representation of domain information and, as such, it must be rigorous. Formal information sources are critical for the construction of the ontology in this scenario. They will establish the terminologies to be used and ensure that it is accurate. There are two types of knowledge resources: non-ontological and ontological resources. For the purposes of ontology specification, non-ontological resource reuse and reengineering is a key element of the NeOn methodology [29]. To perform this extraction of terminologies and key concepts will be extracted from them. The case studies that were used to drive the specification of the framework are subsequently formalized into ontological resources). Attendance management keeps track of students' attendance via their fingerprints. This system records students' attendance by scanning their fingers on the device. As for non-students, the system will reject the fingerprint. The terminology derived is summarized in Table 1.

Table 1. Built environment components.

City	District	Street	Building
• Local Government Information • Population • Address	• Address • List of Buildings • List of Streets • Name	• Has Pavement • Traffic Light • Traffic Level • Pollution Level • Noise Level	• Owner • Address • Postcode • Building • Number

This table has been derived from a study of the relevant literature in paper [9] to form a list of basic concepts that act as a starting point for a set of terminology to feed into the ontology developed. In addition to the study of general terminology, various applications that employ CPS and digital twins in the built environment were studied. These were elicited from the key categories of current digital twin/CPS uses which are energy management, healthcare, transportation and emergency response [30]. In the absence of detailed examples of real digital twin use cases, this thesis utilized use cases of various more common smart systems that are commonly employed as part of a wider digital twin systems: smart parking system and attendance management system (See Table 2). For these use cases, the NeOn methodology is utilized to develop the built environment access management ontology [24].

Table 2. Use cases access control.

Case study 1: Smart Parking System Access Control	
Data Description	**Notes**
The number of parking floors available	The system administrator can configure the number of parking floors. The location's space determines the spot number, and the system administration adds entrance/exit time data based on the organization's operating hours. For instance, there are two parking levels, each with 12 spaces. From 8:00 a.m. to 8:00 p.m., parking spaces are accessible. On each floor, the user can locate a parking space that is open and pay for it hourly. The system administration will change the parking system to make those spaces appear to users as unavailable parking spots when the floor or parking spots are undergoing maintenance work.
Case study 2: Attendance Management System Access Control	
information about the students (who is available in the system)	A new student may be added by the system administrator based on the student's schedule.

5.2. Analysis of Existing Ontological Resources

Access management is a relatively new field that aims to secure digital infrastructures against vulnerabilities or threats [31]. Although knowledge of access management in smart cities issues is primarily held by those in the ICT industry, due to the widespread use of ICT, access management knowledge should be disseminated to the general public [31]. Furthermore, the range of contributions provided by diverse professionals in this sector has steadily established a wide knowledge base of access management across different disciplines. Some of these efforts have led to the development of ontologies to help define, organize and signify a vocabulary of concepts relating to a particular specialism [32]. The NeOn method suggests that pre-existing non-ontological and ontological tools should be reused for the purpose of domain ontology construction. The semantic model produced draws upon ontologies which have been defined and, consequently, is in accordance with alternative tools considered to be context ontological. Efforts have been made to refine the analysis of reusable tools by producing lists of the possible users and uses, as well as by suggesting competency questions. There is the potential for the different concepts dis-cussed for future ontologies to be categorized. As such, a core aspect of the NeOn approach being applied in the current work is to re-use existing ontological resources where possible. A notable advantage of reusing ontologies is the fact that they are preformulated which saves both money and time when developing ontologies. In addition, utilizing pre-existing ontologies adheres to the principle of creating integrated knowledge bases. If those developing ontologies are given free rein, the majority will opt to re-use an existing ontology if it is practical to do so. What follows is a description of the prevailing ontological resources which are known to contribute to the access management ontology of built environments. The ontology reflects the semantic integration required to achieve access management in smart cities. This includes resources and policies but also permission between physical built environment assets, IoT devices that are related to the built environment, cyber–physical systems, current built environment services (smart parking, attendance management, access door system and smart air conditioning system), existing security standards, digital twin and BIM datasets, as well as newly developed user interfaces those who use them.

5.3. Existing Built Environment Ontological Resources

Ontologies for the semantic representation of smart buildings. As a result, this feature of the ontology can be applied to the access management framework in smart cities. To build the ontology in the field semantic landscape, future possible connections with other built environment ontologies may be researched later. The access management in smart cities

concept will be integrated in the built environment application ontology. One of the existing built environment resources that was considered is the CUSP ontology [26]. This particular ontology relates to the semantics required by Cardiff University's CUSP platform which is decision-making tool offering in-depth urban analytics through an en-gaging interface [26]. As this platform is semantically driven, this offers us a great source of existing ontological resources. However, it should be noted that, as a research prototype, currently, the CUSP platform does not have an inbuilt security framework or security-focused semantics.

5.4. Sensing Resources

The semantic description of a sensor, its measurements and the sensing process are described in the ontology. The user should be able to capture the measurements and provenance whether by focusing on performance or measurement. Observation and Measurements ontology (O&M) [33,34], SSN/SOSA ontology [35] and SAREF ontology [36] are recognized frameworks for the semantic modelling of observational data and sensors. The O&M ontology, on the other hand, is restricted because it excludes sensor networks and devices as well as sensing processes. Its main goal is to model "observations, as well as the made relevant in testing when making observations" [37]. SAREF is a model which offers definitions for smart appliances and concrete devices in the built environment [38], in addition to the variables they check. Even though the model includes a comprehensive list of smart appliances and features, its constructivist paradigm is too grounded in factual examples, thereby limiting its applicability when unidentified characteristics are present. The classification of sensors and their observations are included in the SSN ontology at a higher abstraction level, making it the most versatile candidate for the development of the USA ontology. A sensor, for example, in SSN may be any object that detects a phenomenon, from a person to a metering system or a computer program.

5.5. Urban Object Resources

Among the criteria is how objects and individuals are portrayed in urban environments. Consequently, sensors can be attached to certain items and the value they observe is considered to be one of the objects. There are diverse items which are regarded as being urban objects, including buildings, their contents, the purposes served by environments and the individuals who engage in communication with those comprising the community. The buildings and their elements have already been semantically modelled using the ifcOWL ontology [39,40]. IfcOWL is the RDF representation of the Industry Foundation Classes (IFC) standard, which is a data structure and an exchange file format for BIM data [41]. The ifcOWL ontology is a wide ontology with 1230 classes, 1578 object properties and 5 data properties that allow 21,306 axioms and 13,649 logical axioms to be built. This contains, for the best part, the geometries of the existing buildings and lists of Cartesian points, polylines and other similar items [39,40].

5.6. Existing Security-Focused Resources

This research will also seek to integrate existing state-of-the-art semantic resources in the area of security. The primary state-of-the-art security resource is the "NeOn" ontology [24]. In the context of access management, the primary security standard being examined is the OAuth 2.0 authorization "framework." Existing semantic resources in this area include ontology elements of semantics related to a web of things. However, it provides no specific built-environment concepts [24]. The access management ontology has been developed to enable security-based interoperability between physical built environment assets, sensing and actuation devices, BIM and digital twin datasets, prevailing security standards, and the available built environment services. In addition, it facilitates interoperability with regards to user interfaces and those utilizing these interfaces.

6. Validating an Access Management Ontology for Built Environment Cyber Physical System

The validation of the built environment cyber physical systems access management ontology is discussed in this section. This validation will consist of two stages: (1) verification of ontology against competency questions elicited during its development; and (2) technical validation by applying the ontology to a use case deployed on the CUSP Platform. This validation was performed by integrating the access management framework in smart cities and ontology into the existing platform and tested on various case studies operating on a university campus. The remainder of this section will firstly outline the competency questions that were developed and then describe how these are applied to validate the ontology.

6.1. Competency Questions

Competency questions provide a useful means of determining how complex an ontology is owing to the fact that these questions should be answerable using knowledge that is ontology-based [20,25,26,42]. There are five categories of competency questions (security standards, built environment services, actors, built environment data format, IoT devices) that relate to the aspects of smart city access management being integrated by the model. The collection of competency questions concerns the various elements of the built environment such as people, actions and objects and their effect on security efficiency—concepts which must be included in the ontology. Many competency questions are derived and are grouped into the following sections. In total, 42 competency questions are derived.

- IoT devices group questions contain six questions;
- Built environment data format questions contain nine questions;
- Actors' questions contain seven questions;
- Built environment services questions contain eight questions;
- Security standards questions contain twelve questions.

Following the development of the ontology, it is verified against these competency questions. This step of the process entails verifying that all competency questions are answerable via the ontology. This is conducted through a manual comparison of the ontology against the given competency questions [20,43].

6.2. Validation on a University Building

Based on the requirements specification, existing ontological resources and existing non-ontological resources, the access management ontology in smart cities has been developed and validated on two use cases. The university building is a complex use case, with a large mix of individuals that move in and out of the case study dynamically. This includes (a) students, (b) staff, (c) contractors and (d) visitors. This dynamic nature makes it a good case study.

Smart Parking System: makes it possible for staff and students at a university site to make parking reservations and reveal any campus police violations.

Attendance Management System: allows university students to register their attendance and staff to keep track of student attendance.

Figure 3 outlines the classes/properties of the ontology. Due to the large number of classes and properties created and * symbol represents multiplicity, with star indicating any number is valid such as 1, only those from the Smart Parking use case are shown in Figure 3.

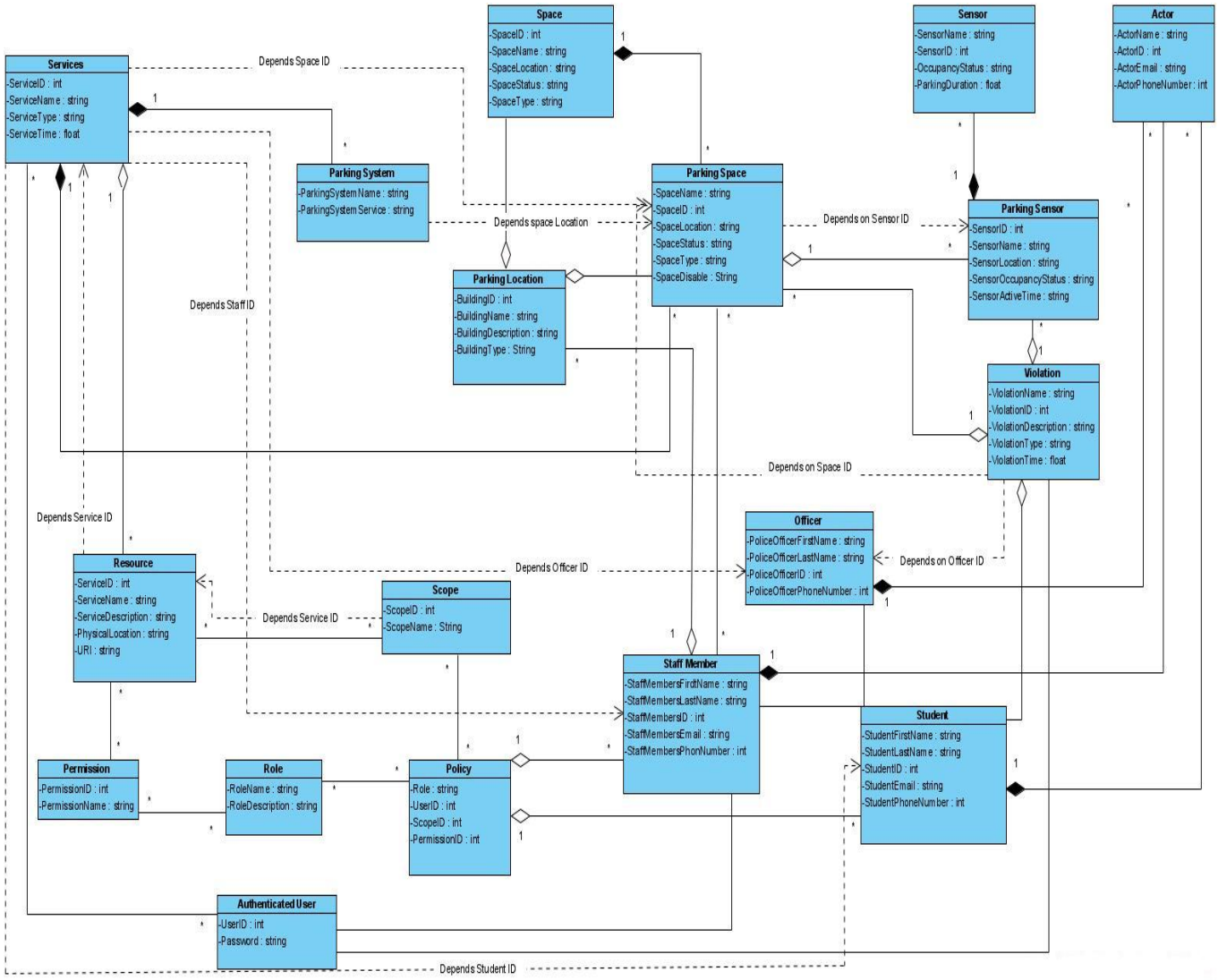

Figure 3. Smart parking system access control.

To perform this validation, a test dataset was created based on an existing dataset of the university campus and surrounding facilities to allow this validation to run in a sandbox environment. The steps involved in creating this dataset are as follows:

- An ontology of the set of surrounding buildings was generated from Open Street Map.
- Ontologies of the university buildings were generated by converting existing IFC models into ifcOWL using commonly available tools.
- Additional data were added manually (extracted from paper-based records) to represent cyber security related information and other metadata that were not present in the BIM datasets.

Once the test dataset was constructed, the validation procedure included the following steps:

(1) The ontology will, indeed, be validated to ensure that it sufficiently represents the security needs of the use case chosen.
(2) The ontology will be validated to ensure that it accurately assigns and provides access rights to built-environment services.

This approach extends beyond authentication to allow users to be granted certain authorizations.

Connecting digital identities (authentication) to access control policies applied to various services, all of which are related to real assets in the case of this use case, and all

users are Cardiff University staff or students. However, users connecting with a digital twin could be from any organization and are verified through their own identity suppliers utilizing single sign-on. However, for presentation in this paper, fabricated names are used. Table 3 provides the social information that presents the users of the smart system services.

Table 3. Identifiers a summary of some users.

User	Roles Given to User
Ahmed (CU Staffmember)	Displaying University Parking Violation
	Reserve University Parking
	Displaying University Parking Violation
	Attendance Recording
	Reserve University Parking
Sara (CU Student)	Reserve University Parking
	Displaying University Parking Violation
Khaled (CU Campus Police Officer)	Record and Display University Parking Violations
Alan (General User)	Not allowed to use digital twin services
Rayan (General User)	Not allowed to use digital twin services

Tables 4 and 5 summarize how these use cases are implemented in the ontology and the roles they are granted. Table 5 identifies the policies defined, documenting the decisions that will be taken to allow/deny access to a given service. Table 5 summarizes the overall validation of the ontology. Here, the individual name represents a list of the things that users can do: Reserve University Parking, Record University Parking Violations, Display University Parking Violations. Table 5 also outlines the authorization results made through utilization of the ontology. Therefore, the results in Table 5 show the ontology is functioning as expected.

Table 4. Policies applied in Cardiff University's Smart System.

Policy Content	Policies	Permissions Assigned	Relevant Service
Allow Staff to Reserve University Parking	Allow if Role = "StaffMember"	Make reservation	Reserve Parking Space
Allow Police Officer to Record and Display University Parking Violations	Allow if Role = "Campus Police Officer"	Record Violation	Record Violation
Allow Staff to Displaying University Parking Violation	Allow if Role = "StaffMember"	Display Violation	Display Violation
Allow Student Attendance Recording	Allow if Role = "Student"	Attendance Management	Attendance Management

Table 5. Policies applied in the university smart system.

Users	Reserve Parking Space	Record Parking Violation	Display Parking Violation	Attendance Recorded
Ahmed	Yes, user is granted access	No, user isn't granted access	Yes, user is granted access	No, user isn't granted access
Sara	Yes, user is granted access	No, user isn't granted access	Yes, user is granted access	Yes, user is granted access
Khaled	No, user isn't granted access	Yes, user is granted access	Yes, user is granted access	No, user isn't granted access
Alan	No, user isn't granted access	No, user isn't granted access	No, user isn't granted access	No, user isn't granted access
Rayan	No, user isn't granted access	No, user isn't granted access	No, user isn't granted access	No, user isn't granted access

7. Conclusions

If smart cities are to provide services that are accessible and holistic, this will require interoperability. Therefore, it is necessary to consider strategies capable of addressing such

matters. Interoperability issues can result when semantics are fragmented across a range of contexts, presenting challenges for integrators and software developers. It has previously been demonstrated that such issues can be effectively addressed by utilizing ontologies which combine diverse semantics across various domains. The access management ontology was devised to facilitate the interoperability of security information among built environment services, sensor devices and assets comprising the physical built environment. Furthermore, it combines user interfaces, digital twin BIM datasets, and security standards. This study has provided insight into various aspects of the topic, including the access management ontology, class diagrams, the re-engineering of built environment non-ontological resources, built environment resources, analysis of pre-existing ontological resources, competency questions, requirement specifications, built environment case studies, the ontology development methodology, and the formation of the semantically specified access management framework. Specifically, the current paper has addressed the following research question:

Can a semantically defined access management framework in smart cities prove suitable to manage the security of smart services deployed in the built environment?

This has been achieved through the specification and validation (on a university site) of the semantically defined access management framework in smart cities. This has shown that the semantically defined access management framework in smart cities can successfully represent the security requirements of smart services operating on a university site and then correctly enforce the defined permissions.

The research limitations of this work and the future challenges it poses are as follows:

Limitation: The case study was performed at a desk study that used produced real ontologies and simulated use of them. This might not be adequate to fully evaluate the functionality of the case study, though. It is therefore strongly encouraged that a live experiment be developed on an actual built environment asset.

Challenges: The challenges and possibilities posed by digital twins in the built environment are identified and described. These problems concentrated on the need to improve current access management procedures in the built environment. This required analyzing the most recent technology in the disciplines of BIM, the Internet of Things, digital twins, smart cities and access management, as well as assessing industry views on access management in the built environment and the barriers to continued progress in this area. While the developed ontology provides a scalable starting point for expansion in additional new use cases, care must be taken to ensure that correct ontology re-use procedures are made, ensuring that existing ontological resources are re-used appropriate as opposed to inventing new and duplicate ontologies.

The present study recommends the following future research areas as a way to further improve access management frameworks for digital twins in the built environment:

Recommendation 1: The validation of the ontology is based on a case study at a university. In the future, the ontology will need to be validated on additional real-world digital twin implementations outside of a managed university environment. This is required for guaranteeing that the platform's final outcomes are secure and dependable.

Recommendation 2: To verify the ontology, evaluate the created access management framework on a larger range of case studies.

Recommendation 3: The creation of new software tools will further demonstrate the access management ontology's promise by enabling safe and scalable data sharing between digital twins and digital twin operators. This will be necessary to enable adequate and safe data sharing across the numerous digital twins that will be needed to represent the future smart cities.

Author Contributions: Conceptualization, K.A. and T.B.; methodology, K.A.; software, K.A.; validation, K.A., T.B. and Y.R.; formal analysis, T.B.; investigation, Y.R.; resources, T.B.; data curation, K.A.; writing—original draft preparation, K.A.; writing—review and editing, T.B.; visualization, R.A.; supervision, T.B.; project administration, K.A.; funding acquisition, K.A. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the Deanship of the Scientific Research, Northern Border University, Arar, Kingdom of Saudi Arabia under grant number NBU-FFR-2023-0066.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA, for funding this research work through project number "NBU-FFR-2023-0066".

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Darif, A.; Chaibi, H.; Saadane, R. Energy optimization of SWIMAC for WSN based on IR-UWB in smart cities by using network coding. In Proceedings of the 4th International Conference on Smart City Applications, Casablanca, Morocco, 2–4 October 2019; pp. 1–5.
2. Kuster, C.; Hippolyte, J.-L.; Rezgui, Y. The UDSA ontology: An ontology to support real time urban sustainability assessment. *Adv. Eng. Softw.* **2020**, *140*, 102731.
3. Howell, S.; Rezgui, Y. *Beyond BIM: Knowledge Management for a Smarter Future*; BRE Electronic Publications: London, UK, 2018.
4. Hashem, I.A.T.; Chang, V.; Anuar, N.B.; Adewole, K.; Yaqoob, I.; Gani, A.; Ahmed, E.; Chiroma, H. The role of big data in smart city. *Int. J. Inf. Man.* **2016**, *36*, 748–758.
5. Contreras, F.R.; Pastor, J.Á.; Losilla, F. A Domain Specific Language for Smart Cities. *Proceedings* **2018**, *2*, 148.
6. Rawat, D.B.; Bajracharya, C. Cyber security for smart grid systems: Status, challenges and perspectives. In Proceedings of the SoutheastCon 2015, Fort Lauderdale, FL, USA, 9–12 April 2015.
7. Demertzis, K.; Iliadis, L.S.; Anezakis, V.-D. An innovative soft computing system for smart energy grids cybersecurity. *Adv. Build. Energy Res.* **2018**, *12*, 3–24. [CrossRef]
8. Alshammari, K. Access Management for Digital Twins in the Built Environment. Ph.D. Dissertation, School of Engineering. Cardiff University, Cardiff, UK, 2022.
9. Alshammari, K.; Beach, T.; Rezgui, Y. Cybersecurity for digital twins in the built environment: Current research and future directions. *J. Inf. Technol. Constr.* **2021**, *26*, 159–173. [CrossRef]
10. Miorandi, D.; Sicari, S.; De Pellegrini, F.; Chlamtac, I. Internet of things: Vision, applications and research challenges. *Ad. Hoc. Netw.* **2012**, *10*, 1497–1516.
11. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [CrossRef]
12. Alelwani, R.; Ahmad, M.; Rezgui, Y.; Kwan, A. Rawshan: Environmental Impact of a Vernacular Shading Building Element in Hot Humid Climates. In Proceedings of the 2019 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Valbonne, France, 17–19 June 2019; pp. 1–6.
13. Ahmad, M.W.; Mourshed, M.; Yuce, B.; Rezgui, Y. Computational intelligence techniques for HVAC systems: A review. In *Building Simulation*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 359–398.
14. Rezgui, Y.; Miles, J. Exploring the potential of SME alliances in the construction sector. *J. Constr. Eng. Manag.* **2010**, *136*, 558–567. [CrossRef]
15. Shin, D.-H. Ubiquitous city: Urban technologies, urban infrastructure and urban informatics. *J. Inf. Sci.* **2009**, *35*, 515–526.
16. Steinmetz, C.; Rettberg, A.; Ribeiro, F.G.C.; Schroeder, G.; Pereira, C.E. Internet of things ontology for digital twin in cyber physical systems. In Proceedings of the 2018 VIII Brazilian Symposium on Computing Systems Engineering (SBESC), Salvador, Brazil, 6–9 November 2018; pp. 154–159.
17. Eckhart, M.; Ekelhart, A. Towards security-aware virtual environments for digital twins. In Proceedings of the 4th ACM Workshop on Cyber-Physical System Security, Incheon, Republic of Korea, 4–8 June 2018; pp. 61–72.
18. Lezzi, M.; Lazoi, M.; Corallo, A. Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Comput. Ind.* **2018**, *103*, 97–110. [CrossRef]
19. Corallo, A.; Lazoi, M.; Lezzi, M. Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Comput. Ind.* **2020**, *114*, 103165. [CrossRef]
20. Vajpayee, A.; Ramachandran, K. Reconnoitring artificial intelligence in knowledge management. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *8*, 114–117.
21. Suárez-Figueroa, M.; Gómez-Pérez, A.; Fernández-López, M. The NeOn methodology framework: A scenario-based methodology for ontology development. *Appl. Ontol.* **2015**, *10*, 107–145. [CrossRef]
22. Hou, S. *An Ontology-Based Holistic Approach for Multi-Objective Sustainable Structural Design*; Cardiff University: Cardiff, UK, 2015.

23. Alshammari, K.; Beach, T.; Rezgui, Y. Industry engagement for identification of cybersecurity needs practices for digital twins. In Proceedings of the 2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Cardiff, UK, 21–23 June 2021; pp. 1–7.
24. Howell, S.; Beach, T.; Rezgui, Y. Robust requirements gathering for ontologies in smart water systems. *Requir. Eng.* **2021**, *26*, 97–114. [CrossRef]
25. Tapia-Leon, M.; Santana-Perez, I.; Poveda-Villalón, M.; Espinoza-Arias, P.; Chicaiza, J.; Corcho, O. Extension of the BiDO ontology to represent scientific production. In Proceedings of the 2019 8th International Conference on Educational and Information Technology, Yantai, China, 10–11 August 2019; pp. 166–172.
26. Hippolyte, J.-L.; Rezgui, Y.; Li, H.; Jayan, B.; Howell, S. Ontology-driven development of web services to support district energy applications. *Autom. Constr.* **2018**, *86*, 210–225. [CrossRef]
27. Chun, S.; Jung, J.; Jin, X.; Seo, S.; Lee, K.-H. Designing an integrated knowledge graph for smart energy services. *J. Supercomput.* **2020**, *76*, 8058–8085. [CrossRef]
28. Beetham, I.F.; Enoch, M.P.; Tuuli, M.M.; Davison, L.J. Stakeholder perspectives on the value of car parking. *Urban Plan. Transp. Res.* **2014**, *2*, 195–214. [CrossRef]
29. Gray, J.A.; Zimmerman, J.L.; Rimmer, J.H. Built environment instruments for walkability, bikeability, and recreation: Disability and universal design relevant? *Disabil. Health J.* **2012**, *5*, 87–101. [CrossRef]
30. Anumba, C.J.; Roofigari-Esfahan, N. *Cyber-Physical Systems in the Built Environment*; Springer: Berlin/Heidelberg, Germany, 2020.
31. Górka, M. Cybersecurity Politics-Conceptualization of the Idea. *Polish Pol. Sci. YB* **2021**, *50*, 71. [CrossRef]
32. Rivadeneira, W.F.B.; Gómez, O.S. Cybersecurity Ontologies: A Systematic Literature Review, ReCIBE. Revista electrónica de Computación. *Inf. Biomédica Y Electrónica* **2020**, *9*, 1–18.
33. Jiang, L.; Kuhn, W.; Yue, P. An interoperable approach for Sensor Web provenance. In Proceedings of the 2017 6th International Conference on Agro-Geoinformatics, Fairfax, VA, USA, 7–10 August 2017; pp. 1–6.
34. Cox, S.J. Ontology for observations and sampling features, with alignments to existing models. *Semant. Web* **2017**, *8*, 453–470. [CrossRef]
35. Pal, S.; Mishra, S.K.; Rath, C.K.; Debnath, N.C.; Sarkar, A. Enrichment of Semantic Sensor Network Ontology: Description Logics based approach. In Proceedings of the 2020 IEEE International Conference on Industrial Technology (ICIT), Buenos Aires, Argentina, 26–28 February 2020; pp. 995–1000.
36. de Roode, M.; Fernández-Izquierdo, A.; Daniele, L.; Poveda-Villalón, M.; García-Castro, R. SAREF4INMA: A SAREF extension for the industry and manufacturing domain. *Semant. Web* **2020**, *11*, 911–926. [CrossRef]
37. Haller, A.; Janowicz, K.; Cox, S.; Lefrançois, M.; Taylor, K.; Le Phuoc, D.; Stadler, C. The SOSA/SSN ontology: A joint WeC and OGC standard specifying the semantics of sensors observations actuation and sampling. *Semant. Web* **2018**, *1*, 1–19.
38. Petrova-Antonova, D.; Ilieva, S. Digital twin modeling of smart cities. In Proceedings of the International Conference on Human Interaction and Emerging Technologies, Virtual, 27–29 August 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 384–390.
39. Pauwels, P.; Krijnen, T.; Terkaj, W.; Beetz, J. Enhancing the ifcOWL ontology with an alternative representation for geometric data. *Autom. Constr.* **2017**, *80*, 77–94. [CrossRef]
40. Pauwels, P.; Roxin, A. SimpleBIM: From full ifcOWL graphs to simplified building graphs. In *eWork and eBusiness in Architecture, Engineering and Construction*; CRC Press: Boca Raton, FL, USA, 2017; pp. 11–18.
41. Pauwels, P.; Zhang, S.; Lee, Y.-C. Semanticweb technologies in AEC industry: A literature overview. *Autom. Constr.* **2017**, *73*, 145–165. [CrossRef]
42. Tarasov, V.; Seigerroth, U.; Sandkuhl, K. Ontology development strategies in industrial contexts. In *International Conference on Business Information Systems*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 156–167.
43. Burov, Y.; Mykich, K.; Karpov, I. Intelligent systems based on ontology representation transformations. In *Conference on Computer Science and Information Technologies*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 263–275.