Access Management for Digital Twins in the Built Environment

By

Kaznah Magbel Alshammari

Supervised by:

Dr Thomas Beach

Prof. Yacine Rezgui

Cardiff School of Engineering
Cardiff University

Cardiff, Wales, United Kingdom

December 2021

Thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy (PhD)

DEDICATION

To my lovely mother’s spirit
whose endless love and care has paved my way to success

To my father
who taught me to be passionate in what I am doing

To my family
for their support and encouragement

ACKNOWLEDGEMENTS

I would like to express my deep and sincere gratitude to almighty God for giving me the energy, time, patience and strength to complete this degree.

I would also like to thank my supervisors and especially main supervisor, Dr Thomas Beach, without whose moral and emotional support while completing my PhD, this thesis would not have been possible. He was always there for me when I was in need. Also, my co-supervisor, Prof. Yacine Rezgui, for his encouragement and great guidance and support during my studies. His expertise and supervision have been of great value to me. Without support from both of my supervisors, this thesis would not have evolved as far as it has. I owe thanks to my colleagues and all of the other staff at the Cardiff School of Engineering for organising many important courses and lectures which were so instrumental in my PhD's progress.

I wish to extend my gratitude to the built environment experts for taking part in the industry survey, which enabling me to meet the main objectives of this study. Their contributions, time, and efforts made this study possible.

I am also grateful to my sponsor, the Saudi Arabian Ministry of Education Northern Border University, for giving me the opportunity to pursue my PhD degree. I wish I could give individual acknowledgments to all of those who have contributed to my work but that would be a tall order. However, I am truly grateful to all of those who have directly participated in this mission.

Finally, I would like to thank my father and my family. Without their encouragement, love and support, I would not have reached so far in my career. I would also like to thank my family and my friends for putting up with me and my mood swings throughout the course of my PhD.

ABSTRACT

Recent technological advances in the built environment have sought to create smart cities by coupling information models such as BIM with Cyber-Physical Systems (CPSs). BIM models are now widely used together with IoT-based systems and embrace smart technologies that provide communication layer compatibility. Digital twins are expected to open new opportunities for cyber-physical systems in the future through monitoring and simulation. Security, on the other hand, is rarely properly considered in this fast-evolving industry.

However, while they provide various advantages, according to the literature, they also present a number of concerns, the most serious of which is security. Attempting to integrate access management into digital twins that will be used in built-environment applications presents significant obstacles. Furthermore, this is an issue that has received too little attention. As a result, digital twins that can safeguard and identify real twins are in demand.

This research focuses on how to enhance the access management frameworks for digital twins in the built environment, paying particular attention to access control, data confidentiality, data integrity, and Single Sign-On (SSO). As a result, this thesis defines an access management framework for digital twins in the built environment that is supported by a requirement specification of access management ontology.

This study engages with built environment experts to consider their role as stakeholders and identifies their main concerns, gauges their assessments of current technologies and utilities, and stimulates public awareness of built environment applications' development goals.

According to these findings, there is still a need for a suitable and safe access management paradigm for digital twins. Those in charge of overseeing smart building investments and the use of BIM in asset design and management must be aware of the latest access management threats and take steps to prevent any risk to the shared data environment.

Therefore, this study has developed a semantically defined access management framework for the built environment through an ontological modelling method which formally represents domain information in the creation stage. This ontology solves the issues identified by previous research and industry surveys by explicitly modelling the relationships in an access management context between physical built environment assets, IoT devices, cyber-physical systems, current built environment services, existing security standards, digital twin and BIM datasets, as well as user interfaces and the actors who use them.

The fundamental novelty of this framework is that while previous work has focused on IoT platforms that integrate with BIM, none of these platforms allow seamless integration with BIM models. The need to be able to operate secure servers appears to have been disregarded in efforts to solve access management problems.

The access management framework is validated using a case study from Cardiff University achieved validating the semantic representation against the competency questions and on data drawn from existing case studies developed on university buildings. The validation has shown that the final access management framework semantic representation satisfies the defined requirements and is suitable for application in various built environment use cases. Furthermore, its functionality is tested in the specified case study, as is its compatibility with the necessary built-environment principles such as SSO.

The key contributions of this study are that it (a) finds the current IoT and CPS security systems to address the access management threats facing digital twins in the context of smart buildings and districts; (b) finds built environment experts to consider their role as a stakeholder and to identify their main concerns; and (c) enhances the access management framework for digital twins in the built environment.

Finally, numerous important recommendations are suggested for future research to help overcome the current study's limitations. These recommendations are designed to stimulate future research in the areas of built environment access management, digital twins, and cyber physical systems.

LIST OF PUBLICATIONS

Journal Papers (published):

- Alshammari K, Beach T, Rezgui Y (2021). **Cybersecurity for digital twins in the built environment: current research and future directions**, ITcon Vol. 26, pg. 159-173, https://doi.org/10.36680/j.itcon.2021.010.

Conference Papers (published):

- K Alshammari, H Li, A Kwan (2019). **Security Model Collaborative Building Design**. *Proceedings of the 36th International Conference of CIB W78, Newcastle-upon-Tyne, UK, 18-20 September, pp. 724-732* (ISSN: 2706-6568), http://itc.scix.net/paper/w78-2019-paper-068. (See Appendix H).

- K. Alshammari, T. Beach and Y. Rezgui, "**Industry Engagement for Identification of Cybersecurity Needs Practices for Digital Twins,**" *2021 IEEE International Conference on Engineering, Technology and Innovation* (ICE/ITMC), 2021, pp. 1-7, doi: 10.1109/ICE/ITMC52061.2021.9570208. (See Appendix H).

- Alshammari, K., Beach, T. and Rezgui, Y., 2021. **Cybersecurity for Digital Twins in the Built Environment: Research Landscape, Industry Attitudes and Future Direction**. *International Journal of Civil and Environmental Engineering*, *15*(8), pp.382-387, Cybersecurity for Digital Twins in the Built Environment: Research Landscape, Industry Attitudes and Future Direction (waset.org). “Best Paper Award” (See Appendix H).

Contents

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

3DES	Triple Data Encryption Algorithm
ABAB	Australasian BIM Advisory Board
AECFM	Architecture, Engineering, Construction and Facilities Management
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AS	Authorisation Server
BAS	Building Automation System
BIM	Building Information Modelling
BPDM	Business Process Description Metamodel
BPMN	Business Process Modelling Notation
CAD	Computer-Aided Drawing
CPSs	Cyber-Physical Systems
CUSP	Cardiff Urban Sustainability Platform
DoS	Denial of Service
DOs	Digital Objects
EBIS	Extending BIM Level 2 to support the IoT and security
ECTP	European Construction Technology Platform
FIPS	Federal Information Processing Standard
FOAF	Friend-Of-A-Friend
GSA	General Services Administration
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
IBAC	Identity-Based Access Control
ICT	Information and Communication Technology
IFC	Industry Foundation Classes
IoT	Internet of Things
M2M	Machine-to-Machine
O&M	Observation and Measurements ontology
OASC	Open & Agile Smart Cities
ORS	Ontology Requirement Specification
PaaS	Platform as a Service
PAS	Publicly Available Specification
PoC	Proof of Concept
QoS	Quality of Service

QUDT	Quantities, Units, Dimensions, and Data Types
RBAC	Role Dependent Access Control
RDF	Resource Description Framework
RFID	Radio-frequency identification
RML	Rule Markup Language
SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition
SGML	Standard Generalised Mark-up Language
SIDMS	Secure Identity Data Management System
SQWRL	Semantic Query-Enhanced Web Rule Language
SSO	Single Sign-On
SWRL	Semantic Web Rule Language
SWS	Semantic Web Services
SWTs	Semantic Web Technologies
UK	United Kingdom
UML	Unified Modelling Language
URL	Uniform Resource Locator
USA	United States of America
VOWL	Visual Notation for OWL Ontologies
W3C	World Wide Web Consortium
WBANs	Wireless Body Area Networks
OWL	Web Ontology Language
WSDL	Web Services Description Language
WSNs	Wireless Sensor Networks
WWW	World Wide Web
XML	eXtensible Mark-up Language

Chapter 1: Introduction

The purpose of this chapter is to provide an overview of this thesis. It begins by describing the research context, focusing on smart buildings, Building Information Modelling (BIM), digital twins, cyber physical systems, and cybersecurity. The discussion then shifts to the study's reasoning and motivation. The chapter continues by outlining the research aim and objectives, as well as the research hypotheses and research questions. Following that, a summary of the methodology underlying the study and the scope of the research is presented. This is followed by an outline of the thesis' structure and the main contributions the research makes to the existing body of knowledge.

1.1 Background

Currently, the construction industry is seeking to create ever-smarter buildings, cities, and districts (Alshammari, Beach and Rezgui, 2021). Such a trajectory relies on continuous advances in Information and Communication Technologies (ICT) to create and exchange information.

Technological developments in recent times have delivered advances in terms of wireless and mobile communications, ever-present connectivity, improved communication speeds and cheaper sensors (Miorandi et al., 2012). Not only has technology become increasingly pervasive but there has also been closer integration between cyber systems and physical infrastructure (Miorandi et al., 2012), more commonly referred to as the Internet of Things (IoT). Falling costs and advances in communication networks have resulted in the rapid uptake of this technology in recent years (Gubbi et al., 2013). Consequently, this presents numerous opportunities for knowledge of the built environment to yield considerable value (Howell and Rezgui, 2018). BIM is an example of an information model in the built environment and has appeared in the Architecture, Engineering, Construction and Facilities Management (AECFM) industry as a new step in the enhanced digitisation of built environment data (Howell and Rezgui, 2018).

However, the legacy formats of BIM and its convoluted modelling paradigms make it ill-suited for use in an IoT setting (Alshammari, Beach and Rezgui, 2021) . As such, adoption of BIM in the IoT setting remains distant at a time when other systems are increasingly utilising lightweight and extensible data schemas in web-native languages (Alshammari, Beach and Rezgui, 2021). Meanwhile, building designs are increasingly required to satisfy a combination of environmental, societal, and economic requirements and, consequently, they are becoming more complex (Alshammari, Beach and Rezgui, 2021). This is apparent from the need to

include the latest construction technologies, procurement paths, construction methods and materials. As such, rather than relying solely on the traditional disciplines such as knowledge of mechanics, architecture, electrics and structures, professional insight must also be sought in areas such as waste, the environment, energy and the IoT (Howell and Rezgui, 2018).

Through the use of open standards BIM can be used in this evolving environment is in a layered model to help visualise and systematically categorise the different elements, paying particular attention to how best to enable knowledge and ICT to improve business services (Shin, 2009). In essence, this involves the use of a sensing layer, a form of communication, as well as facilities to process, store and analyse information (Alshammari, Beach and Rezgui, 2021). Layered on top of this are the application, business, innovation, and governance layers.

Sensor networks have so far concentrated solely on delivering Cyber-Physical Systems (CPSs) communication infrastructure (Alshammari, Beach and Rezgui, 2021). Therefore, the emerging concept of digital twins adds a new dimension to this concept, providing CPSs a new potential outcome in terms of monitoring, simulating, optimising, and predicting the state of built environment assets (Steinmetz and Rettberg, 2018; Eckhart and Ekelhart, 2018).

In this thesis we define the concept of a digital twin as a digital counterpart to a physical object enabling implementation of monitoring, simulation, optimisation and prediction of the condition of an physical asset (Steinmetz and Rettberg, 2018).

Therefore, a virtual replica of a CPS in the form of a digital twin is useful and can assume a significant role in securing a system with continuous feedback to improve personal satisfaction, productivity, and prosperity (Steinmetz and Rettberg, 2018; Eckhart and Ekelhart, 2018).

A primary concern for any users of CPS or digital twins is cybersecurity (Howell and Rezgui, 2018). Cybersecurity is the function of protecting access to devices and services and preventing unauthorised access to data that is kept on these devices and drives CPS services (Howell and Rezgui, 2018).

Cybersecurity is an integral element of the policies, architecture and operations of companies working in the context of the built environment (Lezzi, Lazoi and Corallo, 2018). Being willing to address cybersecurity issues in a positive way is a significant concern for all parties. In addition, cybersecurity strategies should be fully integrated with organisational and IT strategies to maximise the efficiency of the entire output value (Corallo, Lazoi and Lezzi, 2020).

As a result, one of the most pressing issues facing organisations attempting to implement the Industry 4.0 paradigm is cybersecurity (Haag and Anderl, 2018). Industry 4.0 makes use of intelligent, integrated CPS to automate all parts of manufacturing operations (from design and development to supply chain and service maintenance). To put it another way, Industry 4.0 connects manufacturing to data communication technologies which combine product and process data with machine data and allow machines to communicate with one another (Corallo, Lazoi and Lezzi, 2020). As a result, one of the most common types of security utilised by Industry 4.0 is access control which identifies persons based on the authenticity of their credentials that have access to part of a managed system or facility (Corallo, Lazoi and Lezzi, 2020). There is also a clear need to ensure the security of sensors and actuators as well as user centred services.

The potential benefits that can be derived from deploying digital twins and IoT technologies in the built environment are starting to be recognised (El Saddik, 2018). One possible result of the use of these technologies are smart cities wherein ICT is used to enable information to be shared with the public. The benefits are apparent but there is a need to address the associated security threat because it is not currently possible to integrate BIM data and cybersecurity concepts and, therefore, security has thus far been overlooked (El Saddik, 2018).

More specifically, the following research gaps have been identified according to a literature review and industry survey: Howell and Rezgui, 2018; Howell et al., 2017; Synchronicity, 2019; Wang, Sun and Hutchison, 2016; Alshammari, Beach and Rezgui, 2021b:

- BIM standards are not currently compliant with IoT standards in the areas of access management, there are no specific standards governing how IoT related information can be represented within an IFC model. Therefore, BIM standards must be amended to incorporate effective access management concepts. This requires new technological elements governing how information is utilised in information exchanges. Access management must become embedded in digital twins by incorporating IoT-related concepts in information models such as BIM.
- Several IoT platforms e.g., FIWARE (Fazio and Celesti, 2015) integrate with BIM yet none of these offers the ability to integrate seamlessly with BIM models. This is due to the fact that while these platforms utilise BIM models for spatial elements, IoT related information within BIM models are not considered. Efforts to address the access management concerns associated with BIM have seemingly overlooked the need to be able to operate secure servers.
- Incorporating access management into services operating on digital twins in the built environment is highly complex. To enable digital services driven by digital twins, 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 (authorisation and authentication). The complexity originates from the different categories of users wishing to use data and actuate services from digital twins. These digital twins have differing security requirements based not only on the type of the assets, but the scenario of its use and the impact the action on the digital asset will have on the physical asset.

In response to this, this thesis aims to map the future development of the access management landscape of the built environment by examining the current research and subsequently providing a framework of recommendations for the adoption of access management in the built environment. This entails reviewing the latest technology in the fields of BIM, the IoT, digital twins, smart cities, and access management as well as surveying industry attitudes to access management in the built environment and the obstacles to the further development of this area.

1.2 Research description

Smart cities in which ICT, Digital Twins and CPS are utilised to enable information to be shared with the public are one conceivable outcome of the employment of digital twins and IoT technology in the built environment. However, there is still a pressing need to address the associated security issues as outlined in Chapter 2.

The aim of this study is to enhance access management for digital twins in the built environment which will enable the implementation of access control, data confidentiality and integrity, and Single Sign-On (SSO) across built-environment services using digital twin, BIM data and IoT. Thus, this thesis will specify an access management framework, underpinned by the formal specification of access management ontology for digital twins in the built environment to supports it. This formal representation of domain information has been designed and validated on a case study in the built environment using this standard.

Firstly, a comprehensive literature review of current smart buildings has been conducted to identify research gaps. The extensive literature review offers information on research relating to the security of smart city data, the IoT, BIM and digital twin technologies. Initially identified research gaps were then explored further through a participatory survey and the knowledge base was then reinforced to: (a) check adoption of the cyber-physical system regarding the built environment; (b) check adoption of digital twins in the built environment; (c) determine obstacles to the adoption of access management for digital twins/CPS in the built environment.

The survey was distributed through the European Construction, built environment and energy efficient building Technology Platform (ECTP), social media and individual contacts with experts. The survey contained 24 questions (multiple choice and open questions) and was targeted at the built environment and industry professionals with experience of adopting access management for digital twins/CPS in the built environment.

From the survey and the literature review, a series of recommendations were derived to enhance access management frameworks for digital twins, and these are as follows:

- Develop a framework to provide access controls and SSO across built environment services that leverage digital twin and BIM data.
- Enhance BIM standards along with evolving digital twin and future city standards to fully integrate support for IoT and cybersecurity considerations such as encryption and access control.
- Provide training to enhance skills to improve adoption of access management for digital twins/CPSs in the built environment.
- Enhance relevant technology such as the IoT and CPS to improve adoption of access management for digital twins/CPSs in the built environment.
- Develop and specify a reference architecture for security aware applications in the smart built environment to promote adoption of access management for digital twins/CPSs in the built environment.
- Smart grid security to enhance adoption of access management for digital twins/CPSs in the built environment.
- Expand BIM specifications to become IoT-compliant for the adoption of access management for digital twins/CPSs in the built environment.

This research will solve these problems by specifying an access management framework for digital twins in the built environment which will provide guidance for the implementation of access controls, data confidentiality, integrity and SSO across built environment services, leveraging digital twin and BIM data.

This is underpinned by the formal specification of access management ontology for digital twins in the built environment. Through this specification, a formal representation of domain information has been developed and subsequently validated using a case study in the built environment.

1.2.1 Aims, Objectives, Research Questions and Hypothesis.

The aim of this research is to devise an access management framework for digital twins that factors in a range of constituent elements from the physical objects (i.e., the IoT), information models (including BIM), and user-driven services that exploit the digital twin.

Thus, with their increasing adoption, the IoT, CPS and digital twins deployed in the built environment context face increased security risks. Although several IoT platforms e.g., FIWARE (Fazio and Celesti, 2015) link with BIM, none of these provide seamless integration with BIM models. This is due to the fact that while these platforms utilise BIM models for spatial elements, IoT related information within BIM models are not considered.

More specifically, the objectives of the current research are as follows:

1. Understand the current adoption of digital twins and CPS in the built environment.
2. Identify and understand common use cases of digital twins and CPS in the built environment.
3. Identify the key requirements and threats within the built environment domain with regards to access management.
4. Devise a built environment access management model that factors in the multiple levels of complexity of the built environment along with the wide variety of stakeholders.
5. Apply and validate the access management model through its deployment in a real-life scenario.

The research hypothesis tackled by this thesis is:

> *The introduction of a built-environment access management framework adapted to new technological advances will ensure the security and interoperability of built environment digital twins with existing ICT systems in common use today.*

The research questions are as follows:

RQ1: How suitable are the current IoT and CPS security systems for providing access management for digital twins in the context of smart buildings and districts?

RQ2: What are the current obstacles to tackling access management threats to the built environment CPSs?

RQ3: What are the key requirements for a semantically specified access management framework suitable for the built environment?

RQ4: Can the current security processes employed by CPS and digital twins be improved to address the access management requirements of digital twins in the context of the built environment?

1.3 Thesis summary

This thesis has been split into 7 separate chapters. The thesis structure along with an illustration of in which chapter each research questions is answered, is given in Figure 1.1. In this figure, each column has five dots that represent the position of the chapters (Chapter 2 to Chapter 6). If elements of a research question are answered within a given chapter, the dot is replaced by a box including a description.

Chapter 2 provides an extended review of the main aspects and technologies involved in the current research including: (a) BIM, (b) smart building, (c) smart cities, (d) digital twins, and (e) cybersecurity. This chapter also presents the identified research gaps in the access management for digital twins in the built environment.

Chapter 3 describes the methodology adopted in the current research to address the stated research questions. The philosophical stance, approaches and strategies employed are described in detail, providing insight into how knowledge has been gathered. The chapter presents the mixed approaches adopted including participatory action research with a description of the various research projects involved, the collection of data via a survey and the case studies used.

Chapter 4 presents the industry survey conducted to: (a) check adoption of the cyber-physical system regarding the built environment; (b) check adoption of digital twins in the built environment; (c) determine the obstacles to the adoption of access management for digital twins/CPS in the built environment.

Chapter 5 presents an access management framework for digital twins. This chapter describes the framework as an outline of the semantic approach that has been utilised to specify its core concepts. The NeOn approach will be used to explain the ontology engineering. The competency questions are a set of questions that an ontology knowledge base system should be able to respond to. They offer a suitable approach to establish how complicated an ontology is.

Chapter 6 validates the final access management framework using a new case study, firstly validating the semantic representation against the compliance questions previously elicited.

Secondly, its functionality is tested in the given case study and its compatibility with the required concepts for the built environment such as SSO is tested.

Chapter 7 concludes the current study with a discussion and a conclusion of the thesis. It provides the key results of the study and how the research questions are addressed. Remaining constraints are discussed and recommendations for future work to be carried out in this area are described.

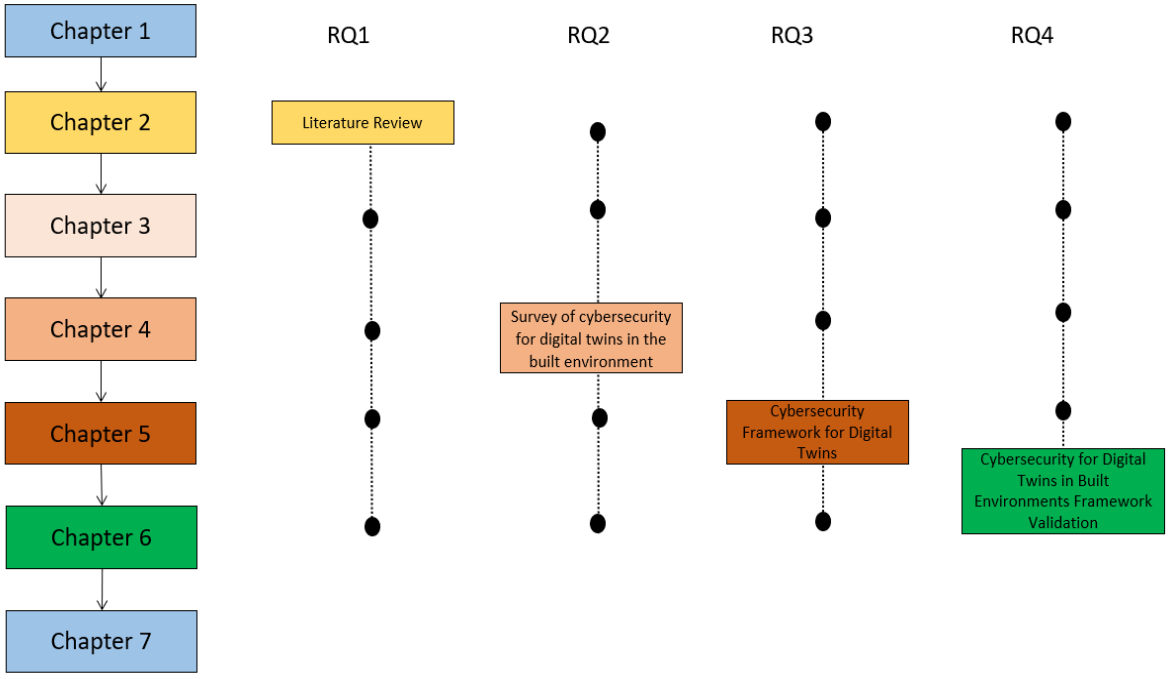


Figure 1.1 Thesis structure

1.4 Summary

This chapter has provided a summary of the subject of this thesis. The scope of the work was first presented by describing key background elements and contextualising the research. Then the hypothesis, research questions, aims and objectives were presented. Finally, a concise description of each chapter was presented to give the reader an overview of the structure of the thesis as well as how each of the research questions map to the key chapters.

Chapter 2: Literature Review

This chapter provides context to the current study by presenting background information and details of the empirical literature relating to the stated research questions. It is based on this empirical literature that it is possible to identify the knowledge gaps that need to be addressed as well as the suitable methodological and technical solutions.

Initially, the chapter reflects on the digital twins, CPSs and BIM tools that are commercially available, revealing the associated shortcomings and the paucity of operative applications. It is possible that the Internet of Things (IoT) or the smart city paradigm could offer solutions and the practicalities are assessed, along with the related security concerns. Secondly, in this chapter, smart cities and other current applications in the built environment are reviewed to illustrate the ongoing efforts in the domain. Also, the key contribution of authentication and the authorisation process is then discussed in smart city applications, as well as how to improve standardisation to enhance the domain's access management and ensure that future secure smart cities can incorporate digital twin and city standards.

*Chapter 2 answers **RQ1:** How suitable are the current IoT and CPS security systems for providing access management for digital twins in the context of smart buildings and districts?*

This chapter will answer this RQ through conducting a review of the main aspects and technologies involved including: BIM, cyber-physical systems and their driving technologies, semantic web technologies, smart buildings, digital twins, cybersecurity and its application in built environment use cases, and existing security approaches in smart cities.

2.1 Building information modelling (BIM)

The architecture, engineering and construction (AEC) industry demands a great deal of collaboration between project users which can only be improved by making the means of communication more secure (Alshammari, Beach and Rezgui, 2021a). This increased security enabling the participants to share confidential information with more confidence improves collaboration. Because the AEC industry depends on the exchange of information, the data files connect by means of exchange files (Das, Cheng and Kumar, 2014; Alshammari, Beach and Rezgui, 2021). BIM data is well-suited for the design, planning and monitoring of progress in the construction of a building because it is updated when users exchange BIM data files (Boyes, 2014; Alshammari, Beach and Rezgui, 2021). BIM was developed within the architecture, engineering, construction, and facilities management (AECFM) industry, causing a marked change in step digitisation. Through Industry Foundation Classes (IFC), BIM can be

created and managed in the design and construction stages, thereby resulting in notable industrial advances (Howell and Rezgui, 2018; Alshammari, Beach and Rezgui, 2021).

BIM concerns the generation and management of information relating to a building over the course of its usable life from the drawing board to its ultimate demolition (Alshammari, Beach and Rezgui, 2021a). BIM shows the basic role in supporting building operation and maintenance by giving an incorporated interface to building operational execution data in all aspects (Mcarthur, 2015; Gha et al., 2017; Alshammari, Beach and Rezgui, 2021).

The benefits of BIM implementation are associated with the BIM process. These advantages include workflow flexibility and the ability to model data integration performance in collaboration. Team members worked on the same model at the same time (Alshammari,Li and Kwan, 2019).

BIM processes are generally implemented as software tool sand the AEC industry uses these tools for both modelling and the communication of project ideas and designs easier (Autodesk, 2003) e.g. Revit (Autodesk), Constructor (Vicosoft) and Microstation (Bentley) (Cha and Lee, 2015; Alshammari, Beach and Rezgui, 2021).

One of the most widely applied BIM standard is IFC (Söbke *et al.*, 2021; Alshammari, Beach and Rezgui, 2021). IFC is an open data model containing specifications for the geometry of building components and related properties used so that people can transfer data from one software program to another when using CAD (Howard, 2008; Alshammari, Beach and Rezgui, 2021). The idea is that it affords comprehensive definitions of the various building components as well as their qualities and inter-relationships. The data used in relation to IFC includes illustrations, numerical models, textual data, structured documents, and the annotations of project managers (Alshammari, Beach and Rezgui, 2021a). IFC appear in ISO standards and are maintained using buildingSMART. The IFC method arguably offers a highly-suitable framework for handling data relating to building management because it has established rules governing areas such as the storage and exchange of data as well as transfer protocols (Howell and Rezgui, 2018; Alshammari, Beach and Rezgui, 2021).

However, it must be noted that neither BIM Level 2 nor BIM models are able to support security features (Alshammari, Beach and Rezgui, 2021a). As such, without modification, the standard specifications cannot be applied to design smart building environments while incorporating security features at the outset of the design process. Instead, it must be incorporated subsequently by means of addition Building Automation Systems (BAS) (Jung, Reinisch and

Kastner, 2012), many of which are proprietary and still do not support the full range of security requirements.

Post design, BIM lays down an array of information that can be used by analysis tools to help steer the commissioning process. Examples of this include when to adjust energy systems and when to undertake the initial evaluation of building performance. The operation stage includes stakeholders who interact with the built environment and some economic activity is produced (Bosch, Volker and Koutamanis, 2015; Alshammari, Beach and Rezgui, 2021). Generally speaking it involves four roles for managing a building: strategy making, controlling, deal-making, and task managing (Alshammari, Beach and Rezgui, 2021a). The operation stage uses 3D or 4D BIM models as a technology to provide data for this stage. In the construction phase, a 4D BIM is often utilised. A 4D BIM is derived from a 3D BIM model and includes a construction project's schedule (Romigh et al., 2017). However, in the operation stage, BIM remains ill-suited for a number of duties, for example, the limitations of IFC with regards to re-using the knowledge of other domains to achieve advanced reasoning (Howell and Rezgui, 2018; Alshammari, Beach and Rezgui, 2021).

2.1.1 Worldwide BIM adoption

The numerous advantages of BIM have prompted many countries to adopt and implement it. This section describes BIM adoption levels in various countries around the world, demonstrating the variability in BIM adoption levels, and then moves on to BIM adoption maturity levels, highlighting the present benefits of and barriers to BIM adoption.

This section presents the top five countries that have the most published work on their BIM adoption: the United States of America (USA), China, the United Kingdom (UK), Germany, and Australia. It also presents details of the progress made in implementing BIM in India; the building sector in India is developing slowly in terms of integrating BIM (Hire, Sandbhor and Ruikar, 2021).

The US has always been the most sustained in its adoption and promotion of BIM (Hire, Sandbhor and Ruikar, 2021). It deployed BIM at all levels of government, from the National University to the local government, resulting in BIM adjustments through time (Amarnath, 2019). It was during 2003 that the US General Services Administration (GSA) created the National 3D-4D-BIM system. As a result of this programme, it became mandatory to apply BIM when undertaking projects for public buildings. In recent years, BIM has emerged as a critical tool in the US Architecture, Engineering, and Construction (AEC) industry (Paul, 2018).

Industrialisation, computerisation, urbanisation and agricultural modernisation, according to China's Ministry of Housing and Urban–Rural Development, have been the main emphasis of China's building industry's expansion with BIM technology playing a key role in each region (Hire, Sandbhor and Ruikar, 2021). China's Tsinghua University has stated that BIM will be the country's future IT solution and the Chinese government has agreed (Hire, Sandbhor and Ruikar, 2021).

Meanwhile, in the UK, in April 2016, the UK government required that all central government-funded projects be delivered with 'complete collaborative 3D BIM' (Hire, Sandbhor and Ruikar, 2021). The adoption of BIM has increased since this requirement came into effect. Based on the National BIM Report 2018, BIM has been embraced by 20% of the industry since the mandate of 2016 (Hire, Sandbhor and Ruikar, 2021). BIM has become a critical aspect for all larger enterprises and it is now affecting smaller businesses as well (State of the Nation Survey, 2021).

A closer look at a highly developed construction industry of Germany reveals that while many construction companies use BIM, it is typically limited to architects and designers and is not necessarily truly collaborative (O'Malley, 2021; Kassem and Succar, 2017).

In Germany, since April 2016, public contracting organisations have had the option of requesting that their contractors use BIM. This holds true for transportation networks, water supply infrastructure, and energy initiatives as well (O'Malley, 2021). Be that as it may, they lack the authority to demand that contractors apply BIM. Outside of the ISO standards, there are currently no specific BIM standard terms for design and construction contracts in use in Germany. The Planen Bauen 4.0 organisation in Germany was created by a number of associations and corporations to actively assist the introduction of BIM in the country (Kalfa, 2018). Official standardisation operations are likewise divided into two tiers, the first of which is represented by the VDI (Association of German Engineers). The group oversees creating legal security standards like VDI2552, as well as the German national BIM standard, which will be authorised by the German Standards Institute – DIN (O'Malley, 2021).

In Australia, the government is committed to allowing and supporting industry and property customers to take advantage of BIM's design, construction, and asset service management capabilities. This strategic framework for BIM in Australia is the first step in establishing a foundation for governments to use a standardised national approach to BIM in large building and infrastructure projects throughout the country. Industry in Australia is also responsible for ensuring that the necessary capability, expertise, and skills are developed. State and territory governments will collaborate with industry to ensure the framework's success, including

continuing to provide collaboration and leadership through the Australasian BIM Advisory Board (ABAB) (ABAB, 2019).

Due to several technological impediments, the Indian construction sector is making modest progress with implementing BIM. Mindset issues, difficulties adapting to repeated design changes, a lack of professionals and skilled resources, software compatibility, high hardware and software costs, a lack of process guidelines, and no government guarantee for BIM implementation are all common barriers (Hire, Sandbhor and Ruikar, 2021).

Even though many nations are embracing BIM, there is still a need for worldwide collaboration in BIM research and development to fully utilise BIM and overcome BIM adoption barriers. Ownership, intellectual property rights and data loss are all significant concerns among countries adopting BIM (Tao and Qi, 2019; Kirstein and Ruiz-Zafra, 2016). However, a notable challenge is being willing to tackle cybersecurity challenges in a constructive light. Based on the analysis of literature, to enhance the efficiency of the total output value, cybersecurity plans should be thoroughly linked with organisational and IT plans. In addition, the potential benefits of embedding digital twin and IoT technologies in the built environment are starting to be recognised and the consequence might be smart cities in which ICT is leveraged to facilitate public information sharing. The advantages are obvious, but the accompanying security issues must be addressed.

2.1.2 BIM maturity levels

Due to the various concepts and levels of BIM adoption, the BIMGroup (2011) developed a model for BIM maturity to clarify expected levels of efficiency as well as trying to support standards and guidance notations and their relationships with one another in terms of how they can be implemented in projects and agreements within the industry (BIMGroup, 2011). The goal of categorising these levels from 0 to 3 types is to enable a concise knowledge and explanation of BIM as well as a knowledge of BIM processes, tools, and techniques. Its main goal is to de-mystify the term ‘BIM,’ making its identification a clear and transparent part of the supply chain, allowing the client to comprehend the supplier chain's offer (BIMGroup, 2011). The BIM maturity levels are depicted in Figure 2.1.

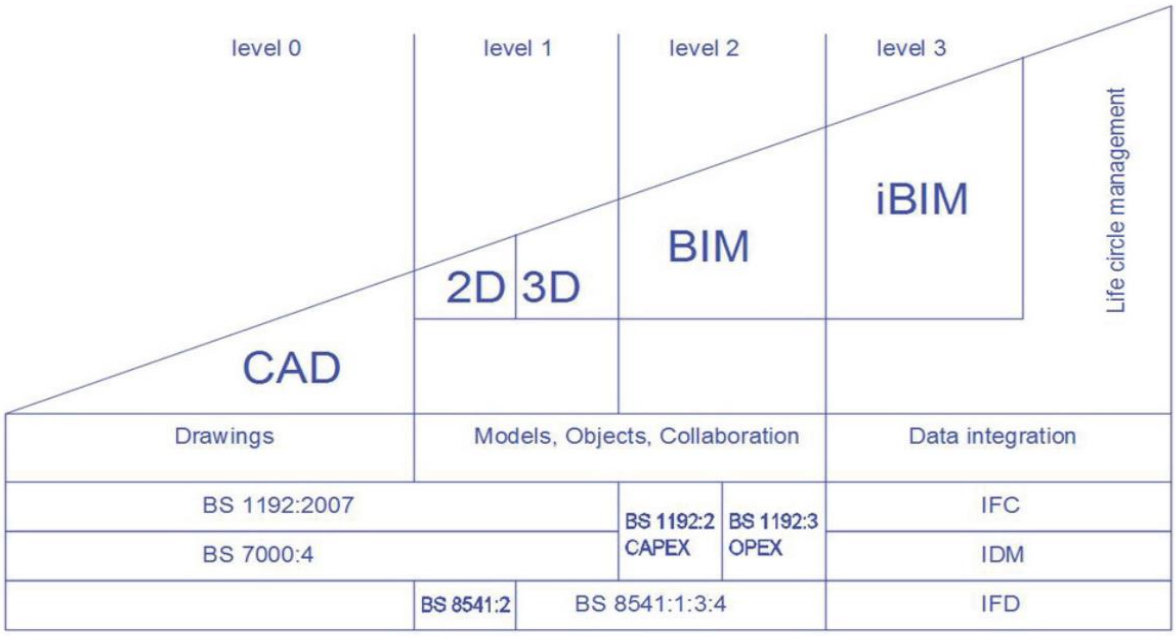


Figure 2.1 *The Bew Richards model of BIM implementation* (Ginzburg et al., 2016)

Level 0: Constructing data in 2D Computer-Aided Drawing (CAD) or possibly unmanaged using paper (or electronic paper) as a potential means of data sharing (Ginzburg *et al.*, 2016).

Level 1: Building data is managed in a 3D virtual environment using 2D CAD. The coordination method is based on the British Standard BS1192: 2007 (BSI, 2007), which provides a shared data environment as well as some standard data formats and shapes. Without any integration, trade data is controlled by independent finance and budgetary control products (Ginzburg *et al.*, 2016).

Level 2: At this level, building data is maintained in a virtual 3D environment with linkages (e.g., relational) to other restraint data sources such as Enterprise Resource Planning (ERP). At level 2, the idea of 'properties' or 'interfaces,' as signified by the label 'iBIM,' is used to integrate heterogeneous (i.e. building and related) information (Ginzburg *et al.*, 2016).

Level 3: At this level, the model is based on open, generally accepted standards and allows building interoperability utilising Web services such as Industry Foundation Classes (IFC) which are managed in a collaborative process in the context of a server, as defined by the BuildingSmart Standards. iBIM is a term that could be used to describe this level (or integrated BIM). It also has the ability to use concurrent engineering methods (Ginzburg *et al.*, 2016).

The level of BIM adoption in the UK construction industry is somewhere between levels 1 and 2 (Prabhakaran *et al.*, 2021). However, to make progress towards level 3 BIM adoption, socio-organisational, legal, technological, and contractual issues must be further enhanced.

Currently, digital twins enable new potential outcomes as far as monitoring, simulating, optimising and predicting the condition of CPSs are concerned (Alshammari, Beach and Rezgui, 2021a). Boje *et al.'s* (2020) study has identified BIM is regarded as a possible starting platform to introduce an evolved three-tier approach to the development of digital twins in the built environment.

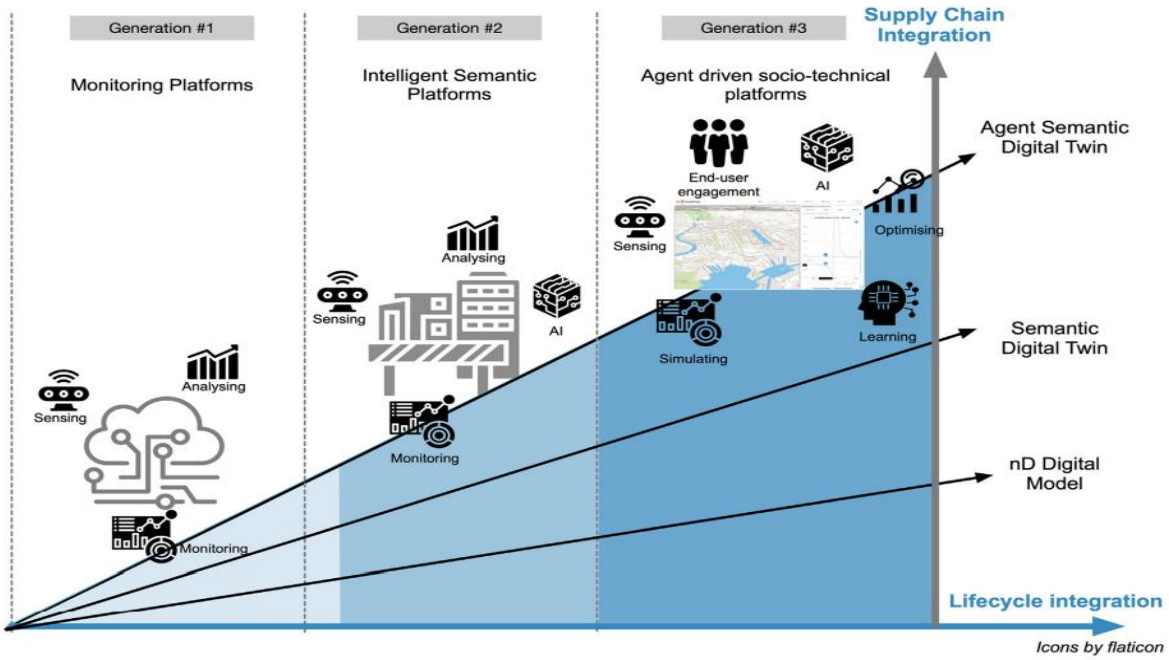


Figure 2.2 *The 3-tier Generation evolution of the Construction Digital Twin* (Boje, Guerriero, *et al.*, 2020)

The three levels described in Figure 2.2 are as follows: *"Generation #1 - monitoring platforms; Generation #2 - intelligent semantic platforms; and Generation #3 - agent-driven socio-technical platforms"* (Candidate, Kelly and Kassem, 2021). The current BIM implementation in this model is to be at the start of Generation #1. This assumption is supported by Boje et al. (2020) who argue that BIM in its current state is unable to deliver the information required throughout an asset lifecycle and, even then, with extensions to its actual abilities, it is unable to perform more complex functions such as prediction and optimisation. In a similar vein, Akbarieh et al. (2020) claim that BIM gives a static representation of an asset's material but a digital twin reflects information acquired over the course of an asset's lifecycle such as state and maintenance information (Akbarieh *et al.*, 2020).

2.1.3 BIM benefits and barriers to adoption

Even though BIM offers significant benefits that have been documented in several building projects, its acceptance and implementation in the construction sector faces a number of challenges and impediments.

2.1.3.1 Benefits of BIM

Applying BIM can benefit an AEC business, through productivity improvements, enabling the production of more detail and useful models. Sari, Wahyuningrum and Kresnanto (2020) identified several benefits of BIM: (a) the presence of a BIM object collection; (b) the capacity to enable dispersed work processes involving different team members working on the one project; (c) the quality of help and accompanying documentation, courses, and other learning tools; (d) the capacity to work on huge projects; (e) a capacity that draws upon numerous disciplines such as structural engineering, architecture, and electrical and mechanical engineering; (f) the capacity to support initial design phase modelling; and (g) direct connection with energy consumption, structural analysis, and project management tools. Other benefits of BIM, as outlined by Naticchia et al. (2020), include: (a) numerous uses for a single data entry; (b) design efficiency; and (c) design base uniformity; (d) conflict resolution and 3D modelling; (e) estimating and take-offs; (f) fabrication and shop drawings; (g) conflict identification; (h) different arrangement and option visualisation; (i) costing mistakes and manufacturing reduction; (j) facilities management.

Other benefits of BIM were described. BIM facilitates the integration of all linked documents and the data generated and required by various disciplines in a project. It also enables rapid control and dispersed access to data, making long-term programming better able to update, maintain and retrieve data. It simplifies resource utilisation by reducing the need for repetitive effort whilst eliminating duplication. It allows for the extracting features and processing of data requiring focused efforts such as cost, area and so on, at any phase of project development. It also makes it simple to switch between alternative representations of the same data which improves visibility and buildability. It reduces conflicts and coordination errors as well as providing the ability to analyse and visualise product quality over the lifecycle of a building with the potential to simplify legal and regulatory processes. Finally, by integrating electronic building objects to manufacturers' websites, it enables the creation of content for them (Hooper and Ekholm, 2010; Doumbouya, Gao and Guan, 2016).

Furthermore, contemporary BIM research in the field of information integration and visualisation reduces job duplication and interface complexity, thereby saving time and money. Nowadays, the BIM capabilities for knowledge transfer, visualisation and parameter optimisation help to reduce the duplication of effort and the complexity of interface integration and this has a favourable impact on construction projects because it saves time and cost (Chuang, Lee and Wu, 2011).

2.1.3.2 BIM adoption issues and barriers

Even though the construction industry is increasingly adopting BIM due to its many benefits and its cost-cutting implications, there are still several impediments and problems that are preventing adoption of BIM in the construction sector. For instance, the construction industry's adoption of BIM is hampered by the fragmented nature of the AEC industry (Eastman and Teicholtz, 2011). Architects are the group most aware of the value of BIM, with 43% estimated to be knowledgeable (Arunkumar, Suveetha and Ramesh, 2018). Only 20% of engineers or contractors have the same level of knowledge as architects. Due to this, there is a widespread perception that BIM adoption is taking much longer than expected due to both technical and management challenges (Wu *et al.*, 2019).

Several factors influence BIM adoption (Ademci and Gundes, 2018) and these can be divided into two categories: (i) technical instruments and functional requirements, and (ii) non-technical strategic problems. There is a need for direction in terms of where to begin, what tools are available, and how to navigate legal, procurement and cultural issues.

Technical challenges (compatibility and dependability), the dispersion of project teams, change reluctance, training shortages, and concerns associated with business processes all present barriers to BIM adoption (Zhao *et al.*, 2015). Furthermore, BIM's legal, contractual and general organisational consequences can be challenging (Eadie *et al.*, 2014). Enshassi, Al Hallaq and Tayeh (2019) divided the obstacles to BIM adoption into three categories: (i) Commercial, in that immediate benefits do not accrue to the primary adopter (designer) and standard BIM contract agreements do not exist; (ii) Legal considerations, such as issues with BIM and issues stemming from how BIM is used; and (iii) technological considerations such as standards, interoperability and archiving. Technical difficulties, BIM usage and deployment management issues, as well as BIM risks have been classified by Wu *et al.*, (2019).

There is agreement that BIM development initiatives should include technical and socio-organisational components (Khudhair *et al.*, 2021). However, there is no general consensus regarding who should own BIM models or who should be responsible for financing and maintaining them during the project lifecycle (Rezgui, Beach and Rana, 2013). There are other socio-organisational, legal and technical challenges that affect BIM (Rezgui, Beach and Rana, 2013) which must be addressed in order for BIM and related technologies to be widely adopted and successful. In the following paragraphs, these topics are discussed in greater detail.

In terms of socio-organisational difficulties, there is a resilient culture of reliance on the publication of legally binding documentation (including technical drawings) in the construction

business (Grilo and Jardim-Goncalves, 2010). The separation of design and construction operations as well as various procurement channels has hampered the integration of construction processes and a building lifecycle in BIM. Small and medium-sized businesses' hegemony in various stages of the lifecycle, particularly during the construction phase, is based on a restricted process, technical maturity, and competencies. Due to narrow project financial constraints, ICT investment is limited (Rezgui, Beach and Rana, 2013). Virtual buildings are connected to rethinking and mapping project authority, responsibilities and financial arrangements and should be included in BIM instead of frozen paper-based work. Because of financial arrangements such as the assessment of contractors when picking items and materials, traditional procurement approaches delay collaboration across the supply chain from the design phase, prohibiting early stakeholder engagement in the design process (Grilo and Jardim-Goncalves, 2011). Clients fund some of the increased costs associated with adopting a BIM method, while others are shared among stakeholders (Bryde, Broquetas and Volm, 2013).

With regards to legal difficulties, it is not always apparent who owns and is responsible for BIM (Das, Cheng and Kumar, 2015). There are no contractual or legal responsibilities for IFC data or IFC-based servers. The most serious of these issues is a lack of specification documentation and contractual drawings (Rezgui, Beach and Rana, 2013). When it comes to resolving disputes, the existing BIM methodology does not include legal responsibilities in the event of insufficient or incorrect information (Kim, Kim and Son, 2013). BIM does not yet follow procurement processes and nor does it address significant challenges to intellectual property rights. The roles, duties and authorities of stakeholders are not inherent in BIM but they can be found in the strict access controls on data which allow for unintentional and unwanted alterations (Beach *et al.*, 2013).

Finally, technological concerns are among the most significant roadblocks because different IFC products can be incompatible (Sebastian, 2011). There has been a loss of semantics between different IFC-based packages during the import/export of IFC (Venugopal and Eastman, 2010). Data fragmentation occurs in BIM among design and engineering teams as well as contractors and facilities managers. Information is continually at risk of being lost due to mergers and bankruptcy and being poorly maintained during the course of a project (Liu *et al.*, 2013). Access controls to data are addressed by commercial and proprietary solutions. Such approaches are inconsistent and fail to incorporate the procedure dimension or project procurement path (Beach *et al.*, 2013). Even though BIM data is housed on a BIM server, security is a concern because it is controlled and operated by a single organisation (Alshammari, Beach and Rezgui, 2021b). When employing virtualised storage to host large

BIM models, there are costs/overheads that affect networks and communications. Data security support, user authentication support, data security support, and access control support are all security limitations that apply when utilising virtualised storage to hold sensitive data (Redmond *et al.*, 2012; Chan, Olawumi and Ho, 2019).

The American Institute of Architects (Rahim, Mohd Nawi and Nifa, 2016) addressed the BIM model ownership issues, suggesting that other legal safeguards and agreements can secure data protection and confidence in the partnering team and these are applicable to a variety of business needs. However, recent research indicates that there are barriers to BIM deployment in UK building practise (Eastman and Teicholtz, 2011) including getting people to grasp the benefit of BIM in order to address their reluctance to change; implementing new work procedures using lean oriented procedures; finding people who understand BIM; becoming trained in BIM; grasping and promoting collaboration, integration and interoperability from across the distribution chain; and construction lawyers and insurers requiring a clear understanding of the different duties of stakeholders brought about by new procedures.

The identified issues could be addressed in several different ways. The technical challenges can include data interoperability challenges, digital data design parameters, and information integration and sharing among BIM model components (Wu *et al.*, 2019). Well-defined transactional construction process models are required to eliminate data interoperability concerns. This establishes the necessary conditions for computing digital data design. It is critical to devise effective techniques for exchanging and integrating data across BIM model elements. Second, because there is no clear agreement regarding how best to apply or use BIM, and because the entire process is not explicitly defined, there is a need to standardise the BIM process and its execution (Wu *et al.*, 2019). The current study intends to address these difficulties which could lead to an increase in BIM use in the AEC market. Managers were formerly limited in terms of their contribution to the planning of buildings, but BIM now allows facility managers to participate in the early stages of the design process. The third and final risk relates to legal difficulties such as BIM data ownership, licencing challenges, and determining who will govern data entry into the model and be accountable for inaccuracies as well as who will update BIM data and ensure its accuracy (Zhao *et al.*, 2015). This may necessitate additional time being spent inputting and analysing BIM data, thereby adding to the design and project management process costs.

As part of this work, the following research gaps have been identified regarding the use of BIM and its relationship to access management:

Research Gap 1: BIM standards need to become compliant with the IoT. In order to do this, BIM standards must be amended to incorporate effective access management concepts.

This requires new technological elements governing how information is utilised in information exchanges. access management must become embedded in digital twins by incorporating the IoT in information models such as BIM.

Research Gap 2: Several IoT platforms e.g., FIWARE (Fazio and Celesti, 2015) integrate with BIM yet none of these offers the ability to integrate seamlessly with BIM models. This is due to the fact that, while these platforms utilise BIM models for spatial elements, IoT related information within BIM models are not considered. Efforts to address access management concerns with BIM have seemingly overlooked the need to be able to operate secure servers.

Research Gap 3: incorporating access management into services operating on digital twins in the built environment is highly complex. In order to facilitate digital services driven by digital twins, there is a need to ensure the protection and identity of real-world services operating using this data through the adoption of access control principles (authorisation and authentication). The complexity originates from the different categories of users wishing to use data and actuate services from digital twins. These digital twins have differing security requirements based not only on the type of the assets, but the scenario of its use and the impact the action on the digital asset will have on the physical asset.

The critical examination of existing BIM contexts has helped to develop a wider understanding of current advances in the field of BIM. It has highlighted worldwide adoption of BIM, BIM maturity levels, the benefits of BIM, BIM adoption issues and barriers, and the future of BIM linking to digital twins.

2.2 Cyber-physical systems and their driving technologies

The importance of information as a tool for dealing with real-world urban concerns such as environmental sustainability, governance, socioeconomic innovation, improved public services, development, and collaborative decision-making cannot be overstated (Khan, Anjum and Kiani, 2013). Smart homes (Cardullo and Kitchin, 2019), transport (Iqbal *et al.*, 2018), grids (Hashmi, Hänninen and Mäki, 2011), healthcare (Demirkan, 2013) and cities (Chourabi *et al.*, 2012; Hashem *et al.*, 2016) are only a few examples of how ICTs are becoming more integrated into daily life. The integration of ICT and the physical world has increasingly been termed 'cyber physical systems.' One primary way of defining a cyber-physical system is *"automated distributed systems that integrate physical reality with communication networks and computing infrastructures"* (Pivoto *et al.*, 2021).

Both CPS and the IoT are networked systems that include physical sensing and/or embedded devices combining physical and digital/cyber elements (Gushev, 2020). The performance of such an approach is determined not only by the quality of the sensors and metres, but also by the consistency and efficiency with which information and knowledge is exchanged (Hashem *et al.*, 2016a). The IoT enables connected objects to communicate via a network that spans the globe, and it is defined as follows:

"a system that deals with the interconnection of "Things". The word "Thing" refers to any physical object that is relevant from a user or application perspective" (Oriwoh and Conrad, 2015).

2.2.1 Core IoT concepts

In the IoT, unique objects things, accessibility, sensing/actuation capabilities, integrated intelligence, interoperability communication capability, self-configurability, and programmability are all significant features (Oriwoh and Conrad, 2015). Figure 2.3 depicts how the IoT works at the municipal level to increase 'intelligence' and create a smart city.

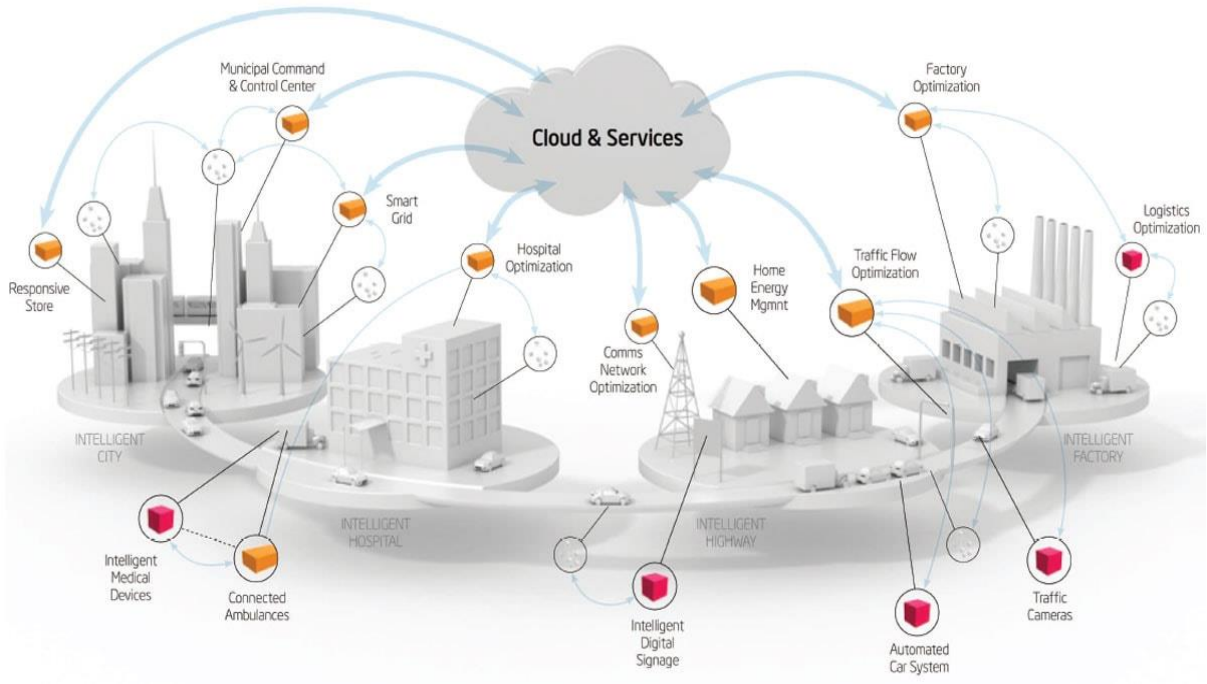


Figure 2.3 *Services made possible by Cloud IoT paradigm* (Rupani *et al*., 2016)

2.2.1.1 IoT phases

The IoT is divided into three phases: collection; transmission; and processing, management and utilisation (Borgia, 2014).

Phase 1: Collection

The detecting and capturing of physical phenomena as well as the distribution of information via hardware devices like sensors and communication devices are all part of the collection phase.

The current section addresses the sensors which effectively serve as the 'things' in the IoT. There is a variety of sensors that monitor sensitive phenomena and provide valuable information about the city. The 'things' can be everyday items in home, entrenched in factory machinery or woven into the fabric of the city. They could be brand-new products and devices created specifically for this purpose.

Smart homes feature smart devices that can track occupancy, the indoor environment, behaviour, activities, and HVAC efficiency among other things (Hancke, de Silva and Hancke, 2013). Intelligent assistants are currently the most frequent smart home gadgets but the industry has the opportunity to grow quickly with applications in control of connected appliances such as lighting, air conditioning and heating or home appliances, smart security using CCTV and sensors for tracking devices, fire and heat monitoring sensors, gas or water leak detection sensors and so on (Sugiharto *et al.*, 2019). Smart entertainment and information devices can also be controlled with multiple interconnected channels.

Smart transportation can monitor traffic flow in real-time, enabling more effective traffic management. With so many forms of transportation and so much data, traffic management is the most difficult aspect of smart transportation (Tahmid and Hossain, 2018; Ijeri, Maidargi and Sunagar, 2020). This involves tracking public transportation, private motorised and non-motorised vehicles as well as the availability of parking spaces, bicycle racks and other amenities. Furthermore, safety is a big concern with road conditions, vehicle speed and road accidents all being relevant factors that fall within the smart transportation umbrella. CCTV, radar, LiDAR and GPS are the most common technologies used. For example, Tahmid and Hossain attempted to control traffic in real-time using digital photographs (Tahmid and Hossain, 2018), whilst others have sought to manage smart parking slots using ultrasonic sensors that identify availability (Khanna and Anand, 2016), Aubry et al. (2014) designed a smartphone application to report traffic violations.

Smart healthcare has two main goals: preventing potential health risks by means of proactive measures and providing improved health services by minimising unnecessary hospitalisations (Papa *et al.*, 2020; Arfi *et al.*, 2021). Smart healthcare services promote a better understanding of healthcare issues and, as a result, help to facilitate treatment personalisation. Furthermore,

cost reduction is a significant incentive for the installation of such systems which is a highly valued advantage in an area where costs are high. Wireless Body Area Networks (WBANs) and mobile apps are examples of smart health technologies that enable the monitoring of an individual's vital signs or health (Chen *et al.*, 2016; Majeed and Aish, 2021). Furthermore, Lemlouma et al. (2013) showed through the use of motion sensors, smart water and energy meters, and/or smart appliances for the assessment of senior autonomy or dependency (Lemlouma, Laborie and Roose, 2013) that some smart home technologies fit into the smart healthcare sector. The use of remote sensing technologies for epidemiological investigations is another example (Sorek-Hamer, Just and Kloog, 2016). Water consumption, quality and leaks are monitored in smart infrastructures as well as the ability to measure key events on the energy network (smart grid), electricity and power consumption, and peak load (Hancke, de Silva and Hancke, 2013). Smart infrastructures also involve the identification of structural faults in buildings, material movement and infrastructure maintenance difficulties. Other applications such as smartPipes that detect leaks with pressure sensing devices (Sadeghioon *et al.*, 2014) or sets of sensors to identify overpass structural deformation for infrastructure health management (Zhang *et al.*, 2016) exist despite the prevalence of publications on smart grids (Hashmi, Hänninen and Mäki, 2011; Lund *et al.*, 2014).

Smart services track citizens' experiences and satisfaction with government services in order to provide the best possible service. Smart services can help with matters such as detecting natural disasters or crimes, monitoring waste volume for collection, and counting facility occupancy (Rehman *et al.*, 2020).

Phase 2: Transmission

The transmission phase includes methods for delivering the gathered data to the various applications and services. It refers to the ‘Internet’ as opposed to the ‘IoT’ which is a network connecting all the different gadgets and allows for the simple and quick transfer of information and knowledge. This network is achievable because it uses cutting-edge communications technology that is becoming more efficient and stable.

Radio-frequency identification (RFID) enables the tags connected to objects to be monitored or traced by means of electromagnetic fields. RFID technology may be used to identify almost anything including animals, clothing and even people (Hashem *et al.*, 2016a).

Wireless Sensor Networks (WSNs) comprise numerous small devices with low power demands. This network has the benefit of being cost-effective and simple to set up as well as providing an excellent potential for device connectivity (Hashem *et al.*, 2016a). The devices

can assess a wide range of environmental and physical parameters as well as act as actuators for control. A wireless system has the advantage of being deployed on a wide scale in a non-intrusive and cost-effective manner which is critical in the smart city concept.

WiFi, ultra-wideband, and Bluetooth are the most extensively used short-range wireless transmission technologies for accessing the Internet or transferring data between devices. They make a valuable contribution in terms of facilitating communication between sensors and the transfer of data (X. Tang *et al.*, 2019).

Standard high-speed wireless communication technologies based on GSM/EDGE network technology include 4G (LTE), LTE-A, 5G. 4G and LTE-A (also known as 4G+). These are currently the most extensively used protocols with data transmission speeds ranging from 100Mbps to 200Mbps. The 5th generation mobile network launched in 2020 with a capacity of up to 10Gbps (Ahmad, 2015). This generation has the benefit of being built to facilitate the IoT by including Machine-to-Machine (M2M) communication.

Phase 3: Processing, managing and utilisation

When all the devices are connected, a considerable amount of data will undoubtedly be generated. The amount of data that needs to be processed and stored has increased dramatically as a result of IoT integration (Khan, Anjum and Kiani, 2013; Vinet and Zhedanov, 2011; Stojkovski and Nenovski, 2020). As a result, cloud computing offers a viable alternative for dealing with such problems (Khan, Anjum and Kiani, 2013; Yamamoto, Matsumoto and Nakamura, 2012).

Cloud computing is defined as: *"a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*" (Hashem *et al.*, 2016; Snaith, Hardy and Walker, 2011).

Among the various types of cloud computing services are Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS). Experts have extensively employed cloud computing to build services (Chen *et al.*, 2016; Arthur, Li and Lark, 2017).

The fog computing paradigm (Dastjerdi *et al.*, 2016) is an alternative to cloud computing that is increasingly being investigated. By incorporating the network's edge, fog computing expands cloud computing capacity and capability. It consists of wide, dense, distributed network edge and datacentres that can service low-latency applications. Furthermore, such

an approach allows data and services provided to the edge and cloud networks to be differentiated, thereby reducing traffic to the cloud. In this case, rather than serving requests submitted by IoT devices in the cloud, requests sent by IoT devices can be served at the network's edge. Finally, fog computing resolves scalability issues by increasing the number of endpoints and minimising cloud processing.

In summary, this phase contains techniques for abstracting bits of information, discovering them automatically and dynamically, and aggregating services from a 'basic' point of view (Borgia, 2014).

2.2.1.2 IoT technical issues

Both Big Data and ICTs are attracting growing interest. Big data's goal (the secure transmission of vast amounts of data in real-time) necessitates the development of increasingly powerful hardware and software. The current system is unable to meet expectations due to technological limitations (Hashem *et al.*, 2016a).

Network architecture: The IoT must overcome some architectural obstacles. With the adoption of a plug-and-play method, the network of associated devices must be adaptable. The architecture must make it simple to integrate new nodes as well as upgrade old ones. It entails complete system interoperability for easy communication between network nodes (Gubbi *et al.*, 2013).

Energy efficiency: Wireless moving sensors do not need to be connected to a power source and must be self-contained. For long-term discontinuous information transfer, the sensors must be energy efficient (Mohammed and Ahmed, 2017). Furthermore, in an ecologically conscious setting, the IoT is only useful if it is constrained by environmental standards that ensure energy efficiency.

Privacy and security: Data containing sensitive information must be safeguarded against potential data breaches. There can have a security issue arising from openly available info, e.g., a traffic data/ cam image help with terrorist planning. Individual privacy, national security and corporate secrets must all be protected (Zhang and Zhu, 2011). As a result, effective services should offer attack resistance, data authentication and client privacy when used on a broad scale (Weber, 2010).

Storage and processing issues: The existing database technologies are insufficient to deal with the amount of data created from numerous sources at a rapid processing pace (Hashem *et al.*, 2016a). The use of the cloud to deal with storage constraints is an area where progress

can be made. However, uploading such a large volume of data will take a long time and this is incompatible with data that changes often (Parashar *et al.*, 2013).

Data integrity: To ensure that big data is used effectively, the system must allow for an 'acceptable' level of incompetence; it must be scalable to handle a large workload; it must be flexible to respond to various queries and operations from diverse data formats; and it must be reliable (Baofu, Hui and Chuansi, 2021).

Quality of service: With a heterogeneous network and a diversity of protocols and technologies, providing the correct Quality of Service (QoS) for the entire network in smart cities is a serious issue (Jalali, El-Khatib and McGregor, 2015). Services should respond to a variety of application requirements without jeopardising the network's stability, flexibility or scalability (Hashem *et al.*, 2016a).

2.2.2 IoT in the built environment

The IoT has introduced innovation as well as unparalleled advantages in terms of convenience and efficacy to many formerly inefficient businesses and processes (Satamraju and Malarkodi, 2020).

In the built environment context, IoT can interconnect each physical entity in a building's construction lifecycle and collects data from the processes of a project (Kagermann, Wahlster and Helbig, 2013; Tao et al*.*, 2014). One way to implement a cyber-physical system in the built environment is to utilise IoT technologies. In current research practice, the building design information model is connected with real-time construction data via integration of BIM with the IoT to enables designers to interact in real-time and resolve construction progress uncontrollability problems and costs during the construction phase of their building (Alshammari, Beach and Rezgui, 2021a). The IoT, sensors, mobile devices and software applications are resources that can be used to better understand the smart construction site. Thus, the interconnectivity and interoperability of the building process are understood from the perspective of both digital world and physical world reconciliation (Ding *et al.*, 2018).

Considering these outcomes and the effect of the IoT on building sites for improving lean construction strategies, the IoT can offer both effective and necessary support. In particular, the measure of data control, the number of specialists included, and the variety of areas to be considered require considerable IoT-empowering highlights (Guerriero et al., 2017).

In addition to use cases within the construction phase, IoT is also seeing use in the design phase of building operation, for purposes such as energy optimisation, and maintenance (S. Tang *et al.*, 2019).

Efforts to safeguard CPS systems have primarily focused on increasing reliability but there is now growing recognition of the necessity to protect against malicious cyber-attacks (Eisenhauer *et al*., 2006; Turk, 2005).

2.3 Semantic Web technologies

Semantic Web Technologies (SWTs) have experienced natural growth in several fields based on CPS. SWTs have been used in smart manufacturing, smart buildings and smart grids and during the engineering and operation of CPSs (Ekaputra, 2020). Thus, SWTs are rapidly becoming a key enabler for digital twins and cyber physical systems.

Tim Berners-Lee outlined a big leap in ICTs in his landmark work "*Information Management: A Proposal*" (Berners-Lee, 1989) which described the notion of hypertext and is now known as that of the "World Wide Web" (WWW). Countless applications have been made available, reflecting the widespread use of the Internet as a WAN that is freely available to all. From there, knowledge may be developed and shared, as well as made publicly accessible to anybody. The WWW has since grown to include social Web and real-time information exchanges, resulting in the production of more data than ever before. During 2017 alone, the total volume of data generated since before the dawn of the digital era increased by 1.5 times (El Bousty *et al.*, 2018), whilst in 2014 and 2015, more data was created than in the entire history of human civilization (Marr, 2015).

As shown in Figure 2.4, the Semantic Web is frequently regarded as the next step in the WWW, also known as Web 3.0. When Tim Berners-Lee first imagined the WWW, he called it the Semantic Web (Nedeva and Dineva, 2015). The DBpedia Linked dataset (DBpedia Association, 2021) essentially converts Wikipedia content into Linked Data and is currently the most striking example of an available connected data resource.

Currently, information is bounded and encoded into distinct formats in the current state of the Web which prevents information from being adequately related. The Semantic Web and the connected data paradigm are founded on the principles of connected data (Ekaputra, 2020). DBpedia had 295 different datasets connected to it as of 2011. In August 2018, the cloud had 1,224 recognised datasets (DBpedia Association, 2021). This exemplifies the participative approach which is one of the Semantic Web's basic ideas. Information sources are reused

and interconnected rather than copied in this new vision, resulting in a realm of information where every bit of knowledge is a singularity.

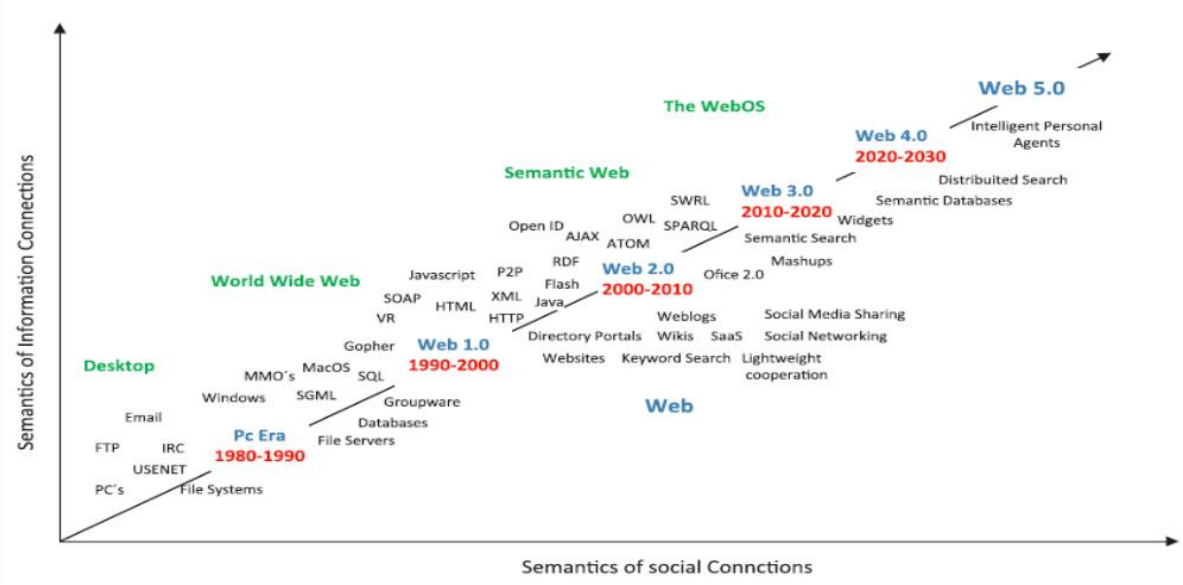


Figure 2.4 *Evolution of the World Wide Web* (Nedeva and Dineva, 2015)

The Semantic Web (Ameri and Patil, 2012) represents the semantics of Web content in a machine-readable structure so as to apply intelligent techniques and automate tasks that are at present dealt with manually by users. Automating tasks are increasingly more significant today for the multiplication of linked devices that are a piece of the IoT (Gubbi et al., 2013).

The Semantic Web includes the following core concepts: (a) ontologies, (b) open standards, (c) ontology languages and (d) semantic web services.

Ontologies are a key factor in the Semantic Web that are used to display and exchange knowledge (Bodenreider and Stevens, 2006). Ontologies should be defined using standard languages to enhance interoperability, information retrieval and natural language processing (Rajput and Haider, 2011).

Open standards; the W3C is regularly engaged in creating and suggesting a variety of rules or particulars for information exchange on the Web. The Semantic Web's core standards include the *"resource description framework (RDF) and SPARQL Protocol and RDF Query Language (SPARQL). RDF is a standard model for data interchange on the Web. SPARQL is a W3C specification and a query language for RDF"* (Abanda, Tah and Keivani, 2013).

Ontology languages: there are several ontology languages such as the Web Ontology Language (OWL) which is regarded as the best ontology language and refers to the

determination of classes, properties and related limitations. OWL is intended for use by applications that need to process the substance of information (Abanda, Tah and Keivani, 2013). Semantic Web Rule Language (SWRL) and Semantic Query-Enhanced Web Rule Language (SQWRL) are propositions for a Semantic Web rule language joining the sub-languages of the OWL (OWL DL and Lite) with the Rule Markup Language (RML). It gives SQL-like tasks to recover information from OWL (Abanda, Tah and Keivani, 2013).

Semantic Web Services (SWS): according to the W3C, a Web service is a software system with the intended purpose of facilitating machine-to-machine engagement across a network. The interface used is referred to as a machine-processible format, otherwise termed the Web Services Description Language (WSDL) (Abanda, Tah and Keivani, 2013).

The utilisation of the semantic web in the built environment is one of the main ways in which BIM technology is progressing. The Semantic Web opens up the option of extending BIM to provide building data consumers with richer and more precisely characterised datasets which are crucial for effective decision-making in the planning, design, construction and operation of built assets (Alshammari, Beach and Rezgui, 2021a).

Adding Semantic Web layers over present Web technologies to enable machines to comprehend the meaning and of data. In the built environment the most commonly utilised form is the ifcOWL ontology (Howell and Rezgui, 2018; Boje, Bolshakova, *et al.*, 2020). This offers several benefits including linking building data to material data, integrating manufacturing data and processes, linking to GIS data, providing context to sensor data, and linking to social data (Howell and Rezgui, 2018) .

Another key development in the built environment is the HyperCat Standard that proposes a REST pattern API into which is a key-based verification strategy is incorporated (Howell and Rezgui, 2018) . The standard also offers further benefits such as *"subscription, more security options, various search methods, a means for further integrating HyperCat into the linked data and Semantic Web ecosystem"* (Howell and Rezgui, 2018) .

2.3.1 Ontologies

A collection of standards produced by the World Wide Web Consortium (W3C) has formalised the Semantic Web, specifying data language and schema, query language, terminology, and identifying potential applications (Semantic Web - W3C, 2021). The idea of ontology, which is one of the key principles of the Semantic Web, can be discovered in those standards. An ontology is defined as descriptions of classes, relationships, functions and other objects, a

specification of a representational language for a shared domain of discourse (Saravana Kumar and Santhosh, 2020).

When discussing computer science, ‘ontology’ is a term that can be somewhat misleading. Indeed, there are numerous levels of interpretation for that phrase, ranging from conceptual to more tangible (Effendi and Sarno, 2018). An ontology can be defined as a set of truths that are accepted as true on a conceptual level. This set of truths is a representation of the real phenomena and, moreover, a specific domain can be rigorously described using an ontology. Organisations, properties and their interconnections are the focus of these statements. This conceptual representation can be defined in a computer-readable format which is referred to as ontologies by computer scientists. As a result, if such computer-readable notions are assumed to be universally true, Artificial Intelligence (AI) can extract more knowledge by implying information from the stated rules(Saravana Kumar and Santhosh, 2020).

It is vital to describe current features such as URI/URL and XML before diving into the definition of ontologies and the standard protocol and languages that support them.

URI stands for Uniform Resource Identifier and is defined as a *“compact string of characters for identifying an abstract or physical resource”* (Dirsumilli and Mossakowski, 2016).They are non-spaced sequences of characters that enable a certain online resource to be targeted. It should not be confused with the Uniform Resource Locator (URL). Indeed, a URL is a type of URI that is distinguished by its location rather than any other characteristics. Hypertext Transfer Protocol (HTTP) and its methods are followed by URLs (Car *et al.*, 2018). It is important to note that HTTP is a set of communication transactions that can be made between a client and a server (usually GET, POST, and DELETE). A scheme (e.g., HTTP) is an authority that identifies the server where a resource is requested, and a path that locates the resource within the server make up the URLs.

Finally, eXtensible Mark-up Language (XML) is an extension of the Standard Generalised Mark-up Language (SGML). These were created to mark-up material in a computer-readable manner with their meta-data (Alameda, 2017).

A Resource Description Framework (RDF) is built on top of XML and URI ideas (see Figure 2.5). RDF attempts to provide machine-readable and intelligible meta-information about resources on the WWW (Schreiber and Raimond, 2014).

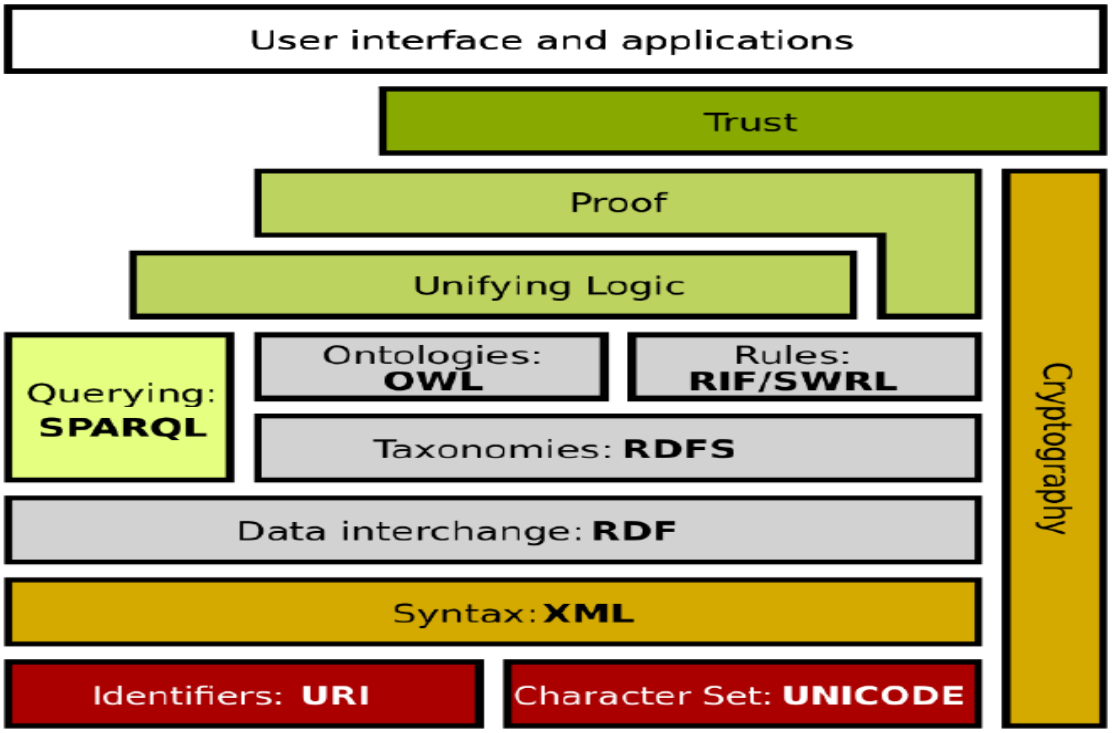


Figure 2.5 *Semantic Web Language stack* (Blasch, 2015)

2.3.2 OWL ontologies

In 2004, the Web Ontology Language (OWL) was released which extended the RDFS functionality to include complete support for the development of ontologies (Bechhofer, 2004). OWL Full, OWL DL, and OWL Lite are the three dialects available. OWL Full is the result of combining the OWL and RDF syntaxes. OWL Full is regarded as being undecidable in terms of reasoning (Pandey, 2012). This is because the expressivity that it enables cannot be reasoned over in a performant way by current reasoners. This is important because, in ontological modelling, reasoning over the knowledge in an ontology is often a key requirement. Conversely the other flavours of OWL can be reasoned over in a performant way. Indeed, an ontology is a logical system with the reasoning ability and infers implicit information from a formally stated knowledge base (Schlagwort, 2011; Murdock and Carroll, 2021). The basic components of such an intelligent system in OWL include conjunction, disjunction, equivalence, universal or existential quantifications, and the ability to establish sub-concept/super-concept associations (subsumptions). Following the amount to which it 'bounds' language expressiveness, the dialect selected to interpret the axioms will deduce information in a different way for a particular graph. The variety of interpretations has an impact on the thinking process. The dialect is unconstrained if it is accessible to too many interpretations; it is undecidable if it is accessible to limitless interpretations.

As a result, reasoning over an OWL Full model is difficult, if not impossible, because OWL Full does not incorporate certain restrictions. To put it another way, OWL Full is far too expressive to suit computational needs. As a result, the OWL DL fragment has also been produced. By adopting Description Logics semantic and adding limits that 'limit' expression to a reasonable degree, OWL DL ensures computational tractability. It distinguishes between object and data attributes and prevents the use of classes as instances. Finally, OWL Lite is a subset of OWL DL that allows the bare minimum of expression, such as cardinality 0/1, inverse, reflexive, and symmetric properties as well as existential (some values from) and global (all values from) constraints.

W3C (W3C Group, 2012) produced OWL 2 in 2009 which was an updated version of OWL. In general, OWL 2 is comparable to OWL 1 but it includes features such as keys, property chains, larger datatypes and range, qualifying cardinality limitations, asymmetric, reflexive and disjunct properties, and increasing annotation capabilities (W3C Group, 2012).

OWL 2 includes a DL fragment, similar to OWL 1, that follows the same concepts as OWL 1. OWL Lite has been altered by the development of three unique fragments or profiles: OWL 2 EL, OWL 2 QL and OWL 2 RL (Carroll *et al.*, 2011). These three profiles are solely applicative in nature and are intended to be chosen in response to the reasoning problems at hand. Indeed, it is interesting to be able to scale down language expressiveness after using an ontology to suit realistic computational needs. When it comes to reasoning over ontologies with a large conceptual component, OWL 2 EL is advantageous because it allows reasoning in polynomial time. In this segment, irreflexive, inverse, symmetric or asymmetric attributes as well as universal quantification, cardinality restriction, disjunction and union as class constructors (unionOf, disjointUnion, dataUnion) are trimmed down. OWL 2 QL is a fragment that handles a large number of cases. It allows querying and reasoning over large datasets in Logspace, regardless of the size of the data. Existential quantified, enumeration of persons and literals, keys, individual equality claims, and negative property assertions are some of the limits in OWL 2 QL. Finally, unlike OWL 2 EL and OWL 2 QL, the OWL 2 RL fragment is designed for applications that require scalable reasoning without sacrificing too much expressivity. The distinction between OWL 2 DL and OWL 2 DL is that construct can only be used in particular syntactic places (Carroll *et al.*, 2011).

2.3.3 *SPARQL*

The SPARQL is a language to enable queries and modifications of RDF graph data in the same manner that SQL allows you to query and modify data in relational databases (Glimm and Ogbuji, 2013; Lehmann *et al.*, 2017). SPARQL supports four basic types of query

methods: SELECT returns resources that match the query; CONSTRUCT returns a RDF graph based on the query; DESCRIBE produces a RDF graph describing the resources queried; while ASK returns a 'true' if the query matches a specific assertion. When querying, the WHERE clause allows you to submit a graph pattern that you want to compare to an existing RDF graph. SPARQL, like SQL, has a collection of expressions that allow for aggregation (GROUP BY, HAVING), sequence and modifier (ORDER BY, OFFSET or LIMIT), algebra (SUM, AVG, MIN, MAX, and so on), string manipulation (CONCAT, REGEX, SUBSTR, and so on), and so on. The SPARQL standard also explains how to analyse a SPARQL query against the various entailment regimes previously mentioned (Horridge and Musen, 2016). Indeed, a SPARQL query for an entailment regime must be built because the answer will vary from one regime to the next (Horridge and Musen, 2016).

2.3.4 Future perspectives

In summary, various attempts have been made in the past 15 years to standardise and use SWTs, particularly RDF, RDFS, OWL and SPARQL with the objective of creating linked data and a unified global system of data.

Despite its potential and exciting advances, the Semantic Web is struggling to gain traction as a mainstream standard (Zaino, 2017). There are still a few hurdles to be overcome before the Semantic Web can see increased adoption (Hassan, 2016): (1) ontologies must be constructed with greater rigour and consistency as well as being sufficiently flexible to be updated; (2) English is the most commonly used language and efforts should be made to create a multilingual system; (3) trust and proof procedures must be included to maintain data credibility and privacy; (4) it must be scalable to meet the future needs of a large implementation, particularly in terms of storage and computing power; (5) security must be strengthened to assure total data privacy and protection; and (6) usability must be enhanced for both users and developers.

In the future, experts predict that the Semantic Web will keep growing and act as a key facilitator of AI, machine learning and data interoperability (Zaino, 2017).

2.4 Smart buildings

Construction projects are benefiting from BIM, especially in terms of how information is delivered across supply chains during procurement and when agreeing a design (Howell and Rezgui, 2018) . By making a distinctive value proposition, BIM can effectively stimulate and re-energise how the construction sector operates by reducing costs and waste while simultaneously making the delivery process more efficient (Howell and Rezgui, 2018).

Moreover, automation and control systems are helping to make buildings smarter because of innovations in the areas of HVAC, telecommunications, building management systems, utilities, and health and safety. It is possible to categorise these as smart building components, pervasive sensing nodes, and intelligent control and actuation devices (Howell and Rezgui, 2018).

Industry 4.0 refers to the integration of industrial technologies with ICT systems that are able to process data and communicate it to create digital twins (Haag and Anderl, 2018; Tao and Zhang, 2017). Digital twins were first used in the aerospace industry (Negri, Fumagalli and Macchi, 2017), paying particular attention to material science, structural mechanics and predictions of performance for aircraft and spacecraft (Tuegel et al., 2011). The digital twin can support information to confirm its continuity during the complete product lifecycle (Dang, Abramovici and Go, 2016; Rosen et al., 2015).

Digital technologies are now being incorporated into the built environment in ways that had not previously been considered and this is giving rise to smart approaches to building and infrastructure management (Howell and Rezgui, 2018). In this domain, BIM is well-suited to offer a particular value proposition if it can be adapted to work alongside Internet-based systems and embrace smart technologies in the form of a learning capability. Continual innovation in the realms of the IoT and artificial intelligence are resulting in more mature products and services that can be applied in an ever-wider range of fields (Howell and Rezgui, 2018).

BIM is used to model built assets and these assets are at the core of a variety of systems that the IoT serves. Therefore, the knowledge at the heart of information models at the design and construction stages sets the background for the data that IoT sensors amass in real-time (Cisco, 2014).

Leverage SWT, BIM information also becomes exchangeable and provides insight into different fields. However, knowledge about trends in the applicability of the Semantic Web is limited (Abanda, Tah and Keivani, 2013).

2.5 Digital twins

The integration of BIM with the IoT can produce a ‘digital twin’ of a real building which can then be used to simulate the construction process, thereby enabling performance to be assessed and the key influential factors to be identified (Tao and Qi, 2019). IoT data is correlated with the BIM model and analytical tools are utilised to simulate the construction process in a synchronous manner (Alshammari, Beach and Rezgui, 2021a). As such, the

combination of real-time IoT data with the BIM model comprises the main element of the enabling technology system. The data made available from the IoT-enabled lifecycle model and the BIM-enabled lifecycle model effectively forms the core of efforts to produce 'smart' construction processes (Tao and Qi, 2019).

Digital twins enable potential new outcomes as far as monitoring, simulating, optimising and predicting the condition of CPSs are concerned. They also have the potential to provide continuous feedback to improve productivity (Steinmetz and Rettberg, 2018). Thus, digital twins enable the synchronisation of the state of a physical asset with a digital replica of the asset and vice-versa. This enables the continuous provision of data enabling the operator of the asset enabling them to monitor the asset and solve problems in real time. Besides, a digital twins useful and can assume a significant role in securing a system (Eckhart and Ekelhart, 2018). Cyber-physical bi-directional data flows offer synchrony that can be exploited so that digital twins offer a more thorough process-oriented and sociotechnical description of what is involved (Boje, Guerriero, *et al.*, 2020). However, there are obstacles, BIM lacks semantic completeness in several areas including; (a) control systems, (b) integrating sensor networks, (c) social systems, and (d) urban artefacts outside of the purview of buildings. True integration of BIM and digital twins necessitates a holistic and scalable semantic approach that takes into account dynamic data at many levels (Boje, Guerriero, *et al.*, 2020).

From a construction standpoint, the digital twin approach aims to improve existing building projects and models as well as their underlying semantics (e.g. IFC) within the sense of a cyber-physical synchronicity wherein digital models are a representation of construction physical assets at a specified period (Tao *et al.*, 2019)

The necessity of monitoring and regulating assets (made elements, buildings, bridges, and so on) throughout their existence, along with technological advancements, has prompted various fields of study to look into digital twin applications and possibilities. Although most of these applications have been studied separately in the BIM sector, the digital twin paradigm necessitates a higher degree of detail and precision which can range from tiny manufactured assets, buildings, urban districts and even national digital twins (Bolton and Enzer, 2018) .

The following are the primary digital twin components (see Figure 2.6) that are considered:

"1) The Physical components, 2) The Virtual models and 3) The Data that connects them" (Boje, Guerriero, *et al.*, 2020).

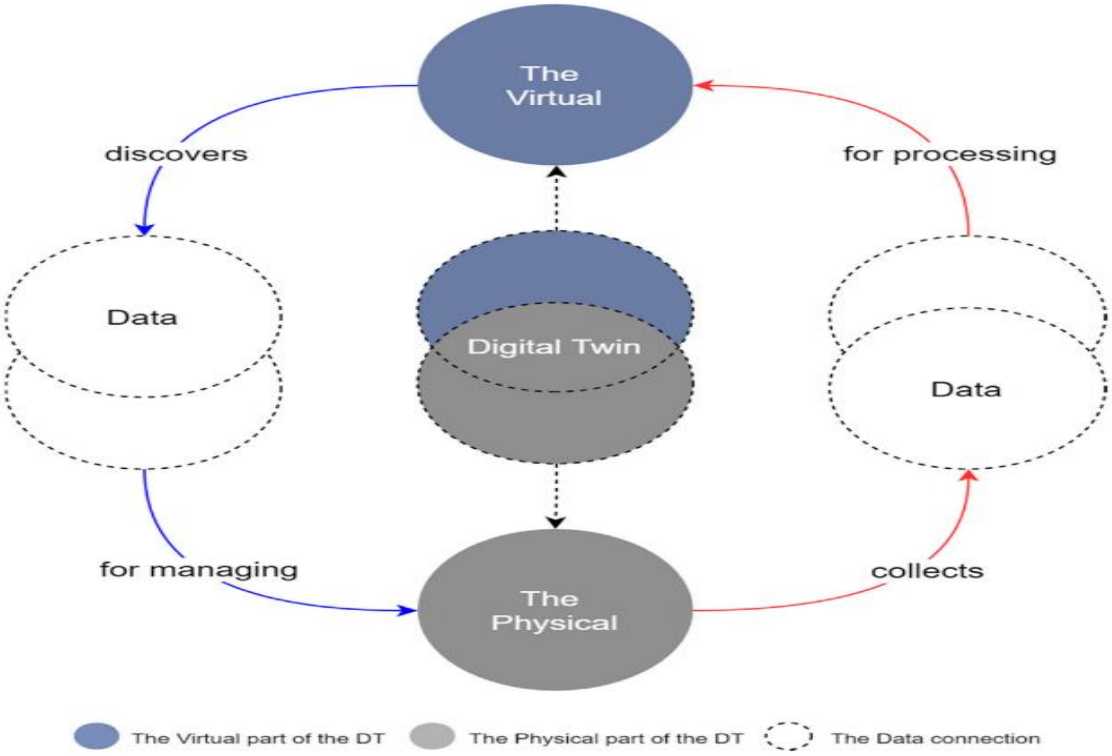
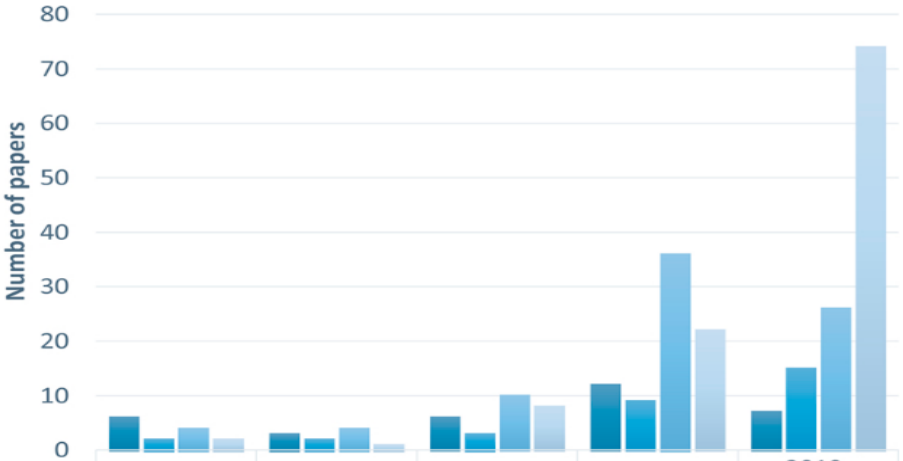


Figure 2.6 The digital twin paradigm (Boje, Guerriero, et al., 2020)

The ‘data’ in its different forms provides the communication loop between the system's ‘virtual-physical’ duality. For example, Grieves (2014) views data from the ‘physical’ to the ‘virtual’ to be raw and in need of processing, whereas data from the ‘virtual’ to the ‘physical’ undergoes multiple transformations. This can be used to process data and store knowledge in digital models with higher degrees of significance. However, data is eventually reflected into the ‘physical’ via actuators. As a result, the ‘physical’ portion collects real-world data before sending it to be processed. In exchange, the ‘virtual’ half uses its embedded engineering models and AI to uncover information that is used to manage the ‘physical’s’ daily operations usage (Grieves, 2014).

Furthermore, 240 scholarly publications relating to digital twin research have been discovered to highlight the digital twin's general development trend. Before 2017, the growth in digital twin research in academic publications was quite gradual However, the number of academic articles on digital twins increased dramatically following 2017. As shown in Figure 2.7, the number of publications relating to the concept, paradigm, and framework, including its digital twin, expanded steadily until 2018 but then began to decline in 2019. Conversely, the volume of literature relating to digital twins and applications has increased year-on-year, with a marked increase in 2019. This shows that the digital twin is progressively emerging from its infancy

into a stage of rapid development with academics starting to investigate real-world behaviours and technologies (Liu *et al.*, 2021).



	2010-2015	2016	2017	2018	2019-2019.9
Concept	6	3	6	12	7
Technology	2	2	3	9	15
Paradigm&Framework	4	4	10	36	26
Application	2	1	8	22	74

Figure 2.7 *Content type of digital twin literatures (*Liu *et al*., 2021)

Cyber-physical system require the capacity to establish the connection between physical and cyber components (Sridhar, Hahn and Govindarasu, 2012). Thus, the security of a CPS relies on sensor network security (Perrig, Stankovic and Wagner, 2004). The majority of efforts expended to ensure the security of sensor networks has concentrated on planning a secure communication infrastructure (Tellez, El-Tawab and Heydari, 2016). The fundamental outcomes contain effective algorithms for: (1) bootstrapping security associations and key management (Eschenauer and Gligor, 2002; Perrig et al., 2002) to create a secure infrastructure; (2) secure communication (Luk et al., 2007); and (3) secure routing protocols (Karlof, 2003; Parno et al., 2006).

A large proportion of the applications are safety critical and if they were to fail, this would have severe consequences, not only for the system but also the people who rely on it (Upadhyay and Sampalli, 2020)). For instance, Supervisory Control and Data Acquisition (SCADA) systems play a central role in various national critical infrastructures including electricity grids, natural gas supplies, transport systems and wastewater treatment systems (Upadhyay and Sampalli, 2020). If these control systems were to be compromised, there would be serious adverse implications in terms of safety, public health and/or the associated financial cost. To date, efforts to secure CPS systems have largely focused on improving reliability but there is

now growing appreciation of the need to protect against deliberately initiated cyber-attacks (Eisenhauer *et al.*, 2006; Turk, 2005).

Sridhar, Hahn and Govindarasu (2012) discussed the importance of cyber infrastructure security with application security to block cyber-attacks. They addressed smart grid cybersecurity: an application that gathers of operational control functions that are important to maintain stability inside the physical power network and its supporting infrastructure. They classified the control loops of the power system that recognise protocols and communication signals, computations, devices, and control actions related to select control loops in the various functional classifications. In this context, control centres receive estimations from sensors that engage with devices in the field. The control centre's algorithms compute the measurements received and take decisions accordingly. Once a decision has been made, it is conveyed to an actuator so that appropriate changes can be made to the devices in the field. As such, there is an opportunity for a third party to identify a vulnerability in the communication system to create attack templates in order to either deny access, cause an extended delay or corrupt the content (e.g., Denial of Service (DoS), timing attacks and desynchronisation) (Huang et al., 2009). The potential for such attacks to the power system must be monitored continually to preserve its integrity. The associated effects could include violations of the system operating frequency, a loss of load, changes in voltage, as well as a range of secondary effects.

By conducting attack studies, it is possible to prepare countermeasures to either minimise the disruption caused by such attacks or stop them from taking place (Alshammari, Beach and Rezgui, 2021a). Examples of countermeasures include attack resilient control algorithms and efforts to detect bad data. Providing an access management layer with both within a possibly this is a future work element between digital twins for the built environment presents a key challenge. Digital twins should be able to secure the identity and protection of their genuine twin. This requires the utilisation of cryptography algorithms.

2.6 Cybersecurity and its application in built environment use cases

The field of cybersecurity combines several different disciplines and is continually evolving. Consequently, it presents notable challenges for those operating in this area. Specifically, cybersecurity is concerned with the technology and people who protect private information associated with people's online activities (Sturdee *et al.*, 2021). External dangers to data repositories are increasing as the amount of sensitive data kept online grows, forcing users to be vigilant about unwelcome intrusions. Cyberattacks pose a significant risk on a global basis (Bada *et al.*, 2019; Taddeo *et al.*, 2019).

2.6.1 Core cybersecurity concepts

Owing to the considerable interest of large corporations in cybercrime, cybersecurity is becoming one of the most competitive disciplines. *"It takes measures to protect a computer or computer system on the Internet against unauthorised access or attack"* (Cains *et al.*, 2021). Studies of vulnerability tests have shown that a CPS cyber incident is an attempt to gain unauthorised access to a system and/or unauthorised access to data within the system. These incidents often arise due to the use of security systems that are out of date or do not properly factor in the complexity of CPS (Kayan *et al.*, 2021).

To control unauthorised access to resources and secure communication across objects, access control technologies have been widely utilised (Gupta and Sandhu, 2021).

2.6.1.1 – Access control

Access control is the refusal or granting of access requests (Gollmann, 2019). It is possible to achieve access control via either the infrastructure that underpins the application or the application itself. It uses generic attributes and operations in an infrastructure (Hu *et al.*, 2013; Gupta, Patwa and Sandhu, 2018).

Discretionary access control regulations, at the resource owner's discretion, grants the right to access protected services to specific user identities, groups and roles. Once a policy is defined, it is necessary to decide if the request satisfies the policy and doing so could require further information to be obtained from a range of sources. Finally, the decision must be forwarded to the component that manages the requested resource. This involves the following steps (Gollmann, 2019):

•Policy Administration Points where policies are set,

•Policy Decision Points where decisions are made,

•Policy Information Points that can be queried for further inputs to the decision algorithm,

•Policy Enforcement Points that execute the decision.

Access control is based on authorisation and authentication. It refers to the blocking of connections by unauthorised persons or devices to the system without authorisation (Corallo, Lazoi and Lezzi, 2020).

Authentication is the main processes for verifying the identity of a user or computer to protect systems from unauthorised access are authentication. Authentication makes it possible to check whether an object's identity is what it is claimed to be. A prevalent authentication method

is to use a password, or other types of authentication approach such as token authentication, biometrics authentication and password authentication (Jiang *et al.*, 2021)

Subsequently, authorisation means the decision that, based on authentication for all other cybersecurity specifications, distinguishes between legitimate and unlawful parties. In the event of a breach, authorisation could result in safety concerns (Ri *et al.*, 2021). Authorisation typically occurs after authorisation on any computer systems that offers differing privileges. There are several types of authorisation currently in use.

Firstly, Role Based Access Control (RBAC) is an architecture for computer systems which, based on privileges, provides users with restricted access after they have passed the required authentication. This model works on a framework based around user functionality and permissions (Jayasankar *et al.*, 2021). Both access control and authentication are rigorously applied for any communication flows. It is important that the solutions feature security measures that can be scaled-up, altered and are robust without interfering with the operation of the grid (Rawat and Bajracharya, 2015; Demertzis, Iliadis and Anezakis, 2018).

In an authorisation system, when an access request is made, security policies are set with respect to the acting principal. If policies refer explicitly to users, the principals are the identities of the users, however principles could also be physical devices or services. In the context of a principle being a user, User identity-based access control is referred to as Identity-Based Access Control (IBAC).

The principal will be a program or service in the event that security policies refer to programs, roles or other such entities capable of issuing requests Generalised (Hu *et al.*, 2013).

Finally, a token records ('encapsulates') the outcome of any judgment on authorisation. In operating systems, for example, the access token provides security keys for a login session. The emphasis is on transmitting the outcome of an authorisation process rather than credentials (Gollmann, 2019).

Based on these two concepts, access management approaches ensure that only relevant users who are correctly identified can access resources (Rawat and Bajracharya, 2015; Demertzis, Iliadis and Anezakis, 2018).

Practical implementations of this approach include the OAuth 2.0 and OpenID Connect protocols. These run directly over HTTP and implement both authentication and authorisation. Among the parties involved in these implementations are the resource/service owner, the server storing the user’s resources, the Authorisation Server (AS) which verifies users, and

the client application that needs to be able to access the resources (Dodanduwa and Kaluthanthri, 2018; Steinleitner, 2020).

Firstly, it is necessary for clients to be registered with the AS. They will obtain the public client ID and client secret which the AS is aware of. Safe sessions are formed between the AS and client based on this secret. Applications requiring authorisation services can then utilise the APIs of the OUATH2 to enable the granting of authorisations which are managed by application ID (known as state in OAuth2). Vulnerabilities in applications using OAuth were introduced by omitting the request ID or using a fixed value (Li, Mitchell and Chen, 2019; Bore *et al.*, 2020).

OpenID Connect adds user authentication back into the flow of OAuth 2.0 messages. In this protocol the authorisation server provides the function of an authorisation and authentication server issuing ID tokens that have been signed digitally. The ID token includes details of the issuer's name and the authenticated user's name (the subject), the strength indicator of the authentication, the nonce accompanying the request for authentication, and the audience (the anticipated relying party), as well as other fields (Gollmann, 2019).

Use of these protocols (among others) enables the implementation of the Single Sign on concept. In this concept, if a user makes use of a single sign on (SSO), they will be granted access to multiple applications and multiple systems with only a single sign on. It is possible to expand such an SSO framework to afford multiple means of access control. A Web-based SSO system can use various Web apps and systems, etc. There is a user interface included that enables the user to access credentials. Every SSO service has an associated web interface enabling SSO services to be accessed via the Internet. In addition, there may be a data manager as part of the Web-based SSO system that supports different types of access policies, openly managing access to data in a range of repositories (Cornwell, 2019).

For SSO, after a single authentication, a user may access multiple services. In addition, the SSO method simplifies the management of the valid users' credentials (Au *et al.*, 2021). The SSO method is convenient because instead of requiring several credential sets (Beltran and Bertin, 2015; Tran *et al.*,2021), a user needs only one set of credentials to access all services. In SSO, access authorisation for services or information is distinguished from user authentication. Authentication is given by IDP and is a utility. After a user is authenticated, an active session is created by the IDP and its information is stored in the user's browser to provide access to other approved services (Radha and Reddy, 2012).

In most web-based implementations of SSO, the OAuth 2.0 standard (Chen *et al.*, 2014) is commonly used. In the SSO context the SAML exchange format is often used to request an access token for OAuth 2.0 as well as performing client authentication. In the SAML-based implementation of SSO (Layouni and Pollet, 2009), there are three key components: *"1) Web Browser of the user; 2) Identity Provider - (often) the authentication server of the user's organisation; and 3) Service Provider - the application software that provides services to the user"* (Ramamoorthi and Sarkar, 2020).

2.6.2 Cybersecurity in the built environment

Cybersecurity is expected to become an integral part of the policy, architecture and operations of companies in the built environment (Lezzi, Lazoi and Corallo, 2018). A notable concern is the ability of organisations to face cybersecurity challenges in a constructive way. This is a catalyst for maintaining the competitive advantage of companies (in terms of economic development and the strengthening of market positions). In addition, cybersecurity strategies should be thoroughly incorporated with organisational and IT strategies in order to maximise the efficiency of the entire value of their output (Corallo, Lazoi and Lezzi, 2020). As such, cybersecurity is one of the greatest problems for businesses involved with the industry 4.0 paradigm. Intelligent, integrated CPSs are used by Industry 4.0 to automate all phases of industrial processes (from design and development to supply chain and service maintenance). In other words, Industry 4.0 ties manufacturing to data communication technologies, integrates product and process data with data from the machine, and allows machines to interact with each other (Corallo, Lazoi and Lezzi, 2020). Therefore, access control is one of the most common types of security that supports CPS in Industry 4.0 which distinguishes individuals based on the authenticity of their credentials to access a managed system or facility. This is a pattern commonly duplicated in built environment applications.

The technological elements that are concerned with cybersecurity manage how data is created, managed and applied as part of information exchanges, across the supply chain and in shared repositories, and common data environments. Construction and asset management supply chains are unaccustomed to accommodating cybersecurity considerations and, as a result, wide-ranging changes will need to be made to security policies if BIM is to be implemented (Boyes, 2015; Roberts *et al.*, 2018). Indeed, the UK government has taken a proactive stance on this matter by encouraging relevant parties to take cybersecurity into consideration, including certification by ISO 27001 contractors (Boyes, 2015).

In the future BIM data will need to drive tools that process data and manage communication with IoT devices. However, this presents key cybersecurity concerns e.g. access management

(Generation and Storage, 2011; Metke and Ekl, 2010). Access management for lots of users who some within utilising digital twins - cyber physical system. some within the organisation of that cyber physical system like staff students. some are not like general public might also want to use digital twins. So, the DT also possess valuable data and can provide real world functionality that's the reason we will need to secure access to the data in digital twins and its actions.

Specifically, cybersecurity in the built environment has emerged as a significant subject. Three fundamental elements of security are discussed here: secure authentication, secure communication, and information security management (Howell et al., 2017). Cybersecurity is based on numerous standards such as ISO 27002:2013, Federal Information Processing Standard (FIPS) 201, Advanced Encryption Standard (AES) (Technology, 2017), and Triple Data Encryption Algorithm (3DES) that provide lower costs while ensuring high levels of security and performance. However, there is a need to apply suitable hazard evaluations and in appropriate scenarios rely on the asset being considered (Howell et al., 2017). Access management frameworks, need to understand:

(a) the type of assets and the level of security required.
(b) The types of users involved and are they known (employs etc..) or unknown (the public) to the digital twin.
(c) The digital services that are to be delivered, and to which users.
(d) The impact that these digital services have on the physical asset.
(e) The level of security required on each digital service.

Howell et al. (2017) identified three avenues to improve security and performance: *"Firstly, research must identify and quantify the risk of a breach of privacy and security to the systemic reliability and quality of service (QoS) caused by insecure authentication occurring in a heterogeneous environment where legacy standards and applications need to remain in operation alongside advanced standards. Secondly, research must identify and quantify loss of data, breach of privacy and vulnerability due to the heterogeneous communication infrastructure (wireless, wired, PLC), and the impact on reliability and QoS. Finally, research must develop guidelines for information security management and inform related legislation and standardisation."*

As BIM is rolled out in the asset management domain, this will result in security matters becoming considerably more complicated (Boyes, 2015) . This is when responsibility for assets is formally transferred to the owner from the project team and asset management

processes are then initiated. This transfer also extends to responsibility for the data incorporated into the BIM model in any common data environments.

Following this handover, the intention is for the model to evolve throughout the working life of the asset, combining data relating to the design and construction stages with that concerning the use of the asset and its maintenance (Boyes, 2015).

However, the standard specifications of BIM Level 2, IFC and COBie cannot support the security features of the IoT. Thus, these standard specifications cannot be applied to assist with building management process for smart built environments that require security and deployment of the IoT. Rather, it has been possible to subsequently incorporate this by means of a Building Automation System (BAS). In short, currently, if a built environment asses is reling upon BIM data for operation, it will be deficient in security and IoT services (Kirstein and Ruiz-Zafra, 2016).While BIM can accommodate conventional aspects of buildings including the likes of doors, ceilings and electrical sockets, it is ill-suited to accommodate security features or IoT devices. For instance, it could not incorporate IoT devices that require a particular security token to operate or determine which individuals are permitted to gain entry to certain rooms (Kirstein and Ruiz-Zafra, 2016).

An integrated solution capable of accommodating security and IoT features was proposed by Kirstein and Ruiz-Zafra (2016). This approach offered the potential for built structures to incorporate dynamic asset data structures. This forms part of the Extending BIM Level 2 to support the IoT and Security (EBIS) initiative which has developed a framework for built environment to incorporate IoT scenarios. This includes details of the procedures to be adhered to and the necessary software tools. This study by Kirstein and Ruiz-Zafra sets out to assign a hierarchical identity to the various physical elements. In essence, this involves each physical asset being assigned a digital representation Digital Objects (DOs) so that the attribute data can be stored in a protected repository, and security features and the IoT can be incorporated in the digital representation. This work utilises the handle system as a registry for persistent identifiers, or handles, for information resources. It also provides the means for resolving handles to locate, access, and otherwise make use of the resources Sun, Lannom and Boesch, 2003). Even though, the global decentralised servers of the Handle System's security only permits access to the local system, it is necessary to be aware that the BIM data could be compromised as a result of security weaknesses in the application-specific servers (Kirstein and Ruiz-Zafra, 2016).

However, this method merely provides a technology base. The BIM PAS 1192-5 standard emphasises that the large-scale publishing of building properties is independent from other

buildings.(Luck and Boyes, 2015). Kirstein and Ruiz-Zafra (2016) validate their work with a Proof of Concept (PoC) in a smart building environment containing two secure rooms to publish the location of these rooms without uncovering details of how they may be accessed or giving undesirable information to potential attackers. Therefore, the technology base provides tools for mitigating threats, but it does not address how they can be used in practice.

Extending BIM Level 2 to support the IoT and Security (EBIS) has ignored another aspect in PAS 1192-5 of Level 2 Standard: the requirement to run secure servers. This contains numerous parts of their operational environment and operating systems (Luck and Boyes, 2015).

In any case, it is necessary to be aware that the BIM data could be compromised because of security weaknesses in the application-specific servers. In addition, relying on external services running on systems with known security frailties could be a vulnerability and, therefore, efforts must be made to ensure they are free from infection. Such an approach to security is necessary for BIM data; it is ignored in EBIS and other projects that are currently planned. (Kirstein and Ruiz-Zafra, 2016).

Those responsible for overseeing investment in smart buildings and the application of BIM when designing and managing assets must have a grasp of the latest cybersecurity threats and mitigate any risk to the common data environment. If this is not the case, the asset's security could be placed at risk and intellectual property could be lost or the systems associated with the asset could be breached. Recognising the seriousness of this issue, the UK government is in the process of publishing a Publicly Available Specification (PAS) setting out how best to manage security issues when applying BIM, managing smart assets or developing digital built environments (Luck and Boyes, 2015).

2.7 Existing Security Approaches in Smart Cities.

In addition to pure academic work, there are currently eight cities engaged in projects to improve their infrastructure using an intelligent solution using ICT to improve the quality and performance of urban services such as transportation, energy, and water (Synchronicity, 2019). Each of these cities have attempted to solve the issue of access management. This section will describe the eight cities and their approaches to security.

These cities are Antwerp, Carouge, Eindhoven, Helsinki, Manchester, Milan, Porto, and Santander. They are all on a path towards developing a smart city based on existing IoT ecosystems and frameworks utilising open standards such as the Open & Agile Smart Cities (OASC) standards.

All of the cities considered have different architectural approaches. These commonly include (a) Southbound interfaces which refer to APIs that support both IoT data collection and command addressing; (b) Data management which refers to data storage and management; (c) Northbound interfaces which provide data access and data management that is provided by context management APIs; and (d) Security and privacy components which refer to security and privacy concepts including authentication, authorisation, and accounting arrangements (Synchronicity, 2019).

Antwerp channels its IoT advancement through two fundamental activities: the Antwerp City Platform as a Service Platform (ACPaaS) and City of Things (CoT).

Carouge looks to use IoT advancement activities in three core architectures: smart parking, street noise monitoring, and an app for tourism that is proprietarily developed and not open.

Eindhoven centres around supporting organic development of and interoperability between the arrangement of IoT stages and vertical systems effectively present in the city. This depends on a wide arrangement of sensors including actuators and wireless communication technologies. The goal in this city is for it to possess four core architectures but only their integrated data management (CKAN) platform is currently available, while FIWARE Orion Context Broker, FIWARE Complex Processing (Proton) and FIWARE Big Data (Cosmos) are currently being evaluated for the next evolution of development.

Helsinki, as of now, is represented by Digitransit architecture (Digitransit, 2019) that implements an Open Message Interface (O-MI) node (Opengroup.org, 2019) and Helsinki CKAN. Manchester is looking more broadly at executing smart city projects, while the current arrangement of smart city projects comprises CityVerve (CityVerve, 2019) and Triangulum H2020.

Each of the smart cities have multiple core architectures. A core architecture is defined as a given project in a given domain. Milan has three core architectures (parking, building/energy, and weather/noise/pollution) that contain several projects in different domains which are specifically developed and not open. Porto is involved with different apps and services which are specifically developed and not open which are: a water management platform, a mobility management platform (Synchronicity, 2019), an environmental monitoring platform, and a citizen platform. The Municipality of Santander provides a large number of projects and IoT initiatives: FIWARE Context Broker (Orion), FIWARE Short Term Historic (Comet), FIWARE persistence connector (Cygnus) and CKAN Data Persistence.

In summary, Eindhoven, Porto and Santander are the most developed urban cities and utilise the IoT. Carouge and Milan each contain three architectures that operate several projects. Antwerp and Manchester are less-developed urban cities with each containing two core architectures (see Fig. 2.8).

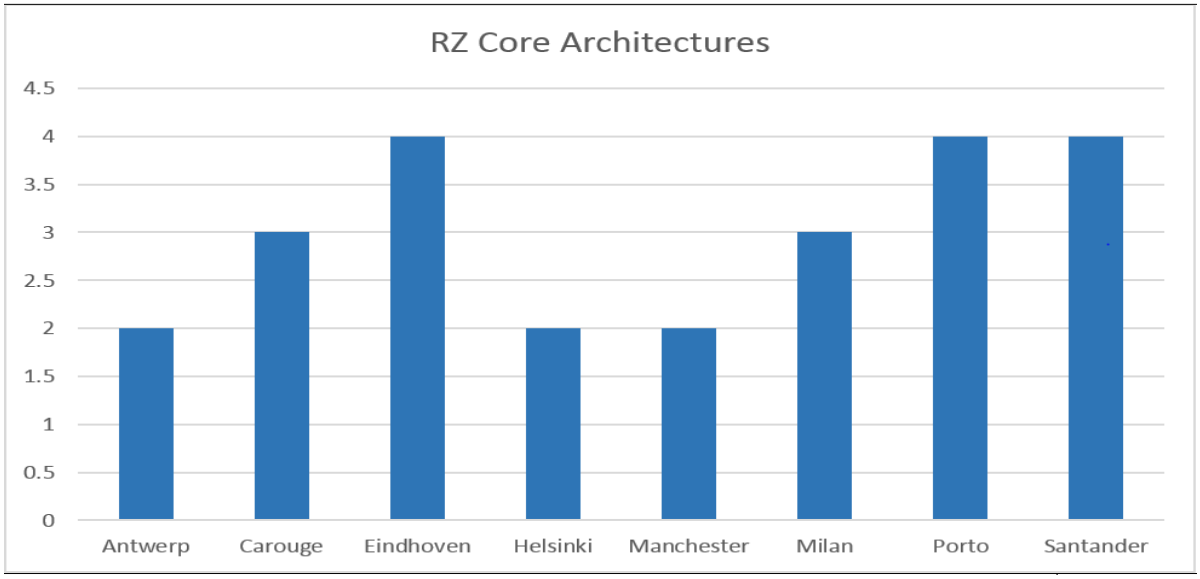


Figure 2.8 Reference Zone Core Architectures

Reference Zones are intended to support various security and privacy levels in future by using FIWARE on FIWARE secure. FIWARE is a cloud platform that gives new novel programming components accessible through APIs to give developers new significant cloud platform operations (Fazio and Celesti, 2015). For smart cities, it offers elements that facilitate data collection from numerous remote systems and IoT devices across the city. In addition, FIWARE offers the means to link conventional open data with real-time data. However, the security component used by FIWARE is a standard off-the-shelf tool and possesses no specific built environment security concepts (Synchronicity, 2019). The Reference Zones are suggesting the creation of a security layer as follows:

Table 2.1 Reference Zone Access Management (Synchronicity, 2019)

Reference Zones	**Access Management layer**
Antwerp	Does not have an official security layer but Antwerp's platforms have been given certain tools to execute authentication and authorisation functionalities.

Carouge	Currently undertaking an investigation into selecting a solution for authentication, authorization and accounting and is considering employing FIWARE AAA with the FIWARE Secure Catalogue as a conceivable solution. The integration of the Carouge IoT with FIWARE will be overseen by Mandat International (International, 2019) and UDG.
Eindhoven	Considering the utilisation of FIWARE in order to improve security and privacy.
Helsinki	Suggests potential support for O-MI security models that execute authentication and authorisation mechanisms operated with the O-MI RESTful API.
Manchester	Manchester public sector IG specialists and private sector partners are looking to implement a privacy management software tool. Privacy Policy Manager (PPM) is being implemented by British Telecommunications (BT) as part of the CityVerve project. Manchester has an API management system that uses an OAuth2 protocol to manage Identity Management (IDM) and an authorisation component.
Milan	Will assess the adoption of FIWARE to enhance certain security and privacy aspects.
Porto	Porto's app is based on login/password through https and is looking for authentication, authorisation and accounting using OAuth/OAuth2. However, no security layer is currently specified.
Santander	There is no official layer specific for security and privacy functionalities in the Santander Reference Zone but it executes some solutions founded on FIWARE Keyrock IDM and Wilma PEP that supports OAuth mechanisms to manage access to resources.

This summary tells us that many of the cities have considered access management. However, the approaches taken by the cities are ad-hoc and they still lack a unified access management model to be able to work suitably and safely (Synchronicity, 2019).

2.8 Summary

The critical study of existing built environment contexts has made it possible to gain a thorough understanding of ongoing trends in the field of industry. It has emphasised the rate of smart city adoption, CPS applications in industry projects, the advantages of adopting IoT and distributed twins as well as the associated obstacles. It has explored the principles that guide the approach to access management and critically reviewed the eight existing creative urban cities in Europe that have been at the forefront of IoT advances.

This chapter has answered ***RQ1:*** *How suitable are the current IoT and CPS security systems for providing access management for digital twins in the context of smart buildings and districts?*

It has found that current security approaches are not suitable in the context of smart buildings and digital twins. Specifically, this review has found that;

- BIM standards are not currently compliant with IoT standards in the areas of access management, there are no specific standards governing how IoT related information can be represented within an IFC model. Therefore, BIM standards must be amended to incorporate effective access management concepts. This requires new technological elements governing how information is utilised in information exchanges. Access management must become embedded in digital twins by incorporating IoT-related concepts in information models such as BIM.
- Several IoT platforms e.g., FIWARE (Fazio and Celesti, 2015) integrate with BIM yet none of these offers the ability to integrate seamlessly with BIM models. This is due to the fact that while these platforms utilise BIM models for spatial elements, IoT related information within BIM models are not considered. Efforts to address the access management concerns associated with BIM have seemingly overlooked the need to be able to operate secure servers.
- Incorporating access management into services operating on digital twins in the built environment is highly complex. To enable digital services driven by digital twins, 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 (authorisation and authentication). The complexity originates from the different categories of users

wishing to use data and actuate services from digital twins. These digital twins have differing security requirements based not only on the type of the assets, but the scenario of its use and the impact the action on the digital asset will have on the physical asset.

Chapter 3: Research Design and Methodology

This chapter introduces the methodology adopted in this research. The paradigm, philosophical stance, research approach and strategies employed are described in detail, proving insight into how the research will be conducted.

The current chapter presents a background to the research paradigms and then describes the paradigm and philosophy selected for this study. It then sets out the hypothesis and research questions and describes the phases of this study and how each will contribute towards answering the research questions. Within the description of each phase, the research instruments that are used will be described and justified.

3.1 Research paradigm background

Research is a systematic analysis that uses disciplined strategies to address questions and resolve issues. The ultimate objective is to develop, re-establish and expand the body of knowledge (Saunders, Lewis and Thornhill, 2019). Lee and Lings (2008), however, state that research concerns knowledge generation about what the authors think the world is. Ponelis, (2015) pointed out a number of reasons for conducting research: (a) to find out what is going to happen in order to resolve possible problems; (b) to discover proof to inform practice; (c) to gain a thorough grasp of how people and the wider world operate; (d) to contribute to personal needs; (e) to test or refute a theory; (f) to find a better way to resolve a problem; (j) to understand the opinions of other people; (k) to generate more interest in the field of research. A particular research paradigm establishes the researcher's world-view and the epistemological position that the researcher takes (Saunders et al., 2009). As a result, it is extremely important that the researcher has a clear understanding of the research paradigm underpinning their research (Hines, 2000). In information technology and construction, many research paradigms can be used to deliver new understandings of real-life problems and issues. Research paradigms are patterns of beliefs and practices that govern inquiries through the provision of lenses, frames and procedures through which investigations are carried out within a discipline (Weaver and Olson, 2006).

Positivism and interpretivism paradigms have commonly been used, gaining researchers' approval as being highly useful for viewing the world of information inside ICT and built environments (Ponelis, 2015; Fellows and Liu, 2015). This is because positivism focuses on studying the natural/physical environment in which we live and work but when it comes to the social world, interpretivism is primarily used, being concerned with the social meaning of an information system in information system science. In addition, most ICT and constructed

environment researchers focus on ‘proof-of-concept-demonstration’ which goes beyond the design and development of information technology objects (Ponelis, 2015).

3.1.1 Positivism paradigm

Positivism was conceived as the study of social reality using the conceptual context, observation and calculation methods, statistical analysis tools, and natural science inference processes (Corbetta, 2013). The conceptual structure is defined by ‘natural law’ categories, cause and effect, empirical verification, description, etc. The observation and evaluation methods involve the use of quantitative variables, the ideological direction of measurement techniques, mental capacities, and psychological states (Corbetta, 2013). Mathematical research includes the use of mathematical and statistical models. In the natural sciences, the inference procedure refers to the inductive process which entails extrapolation to the whole population from a research sample. Positivism emphasises the empirical method used in the natural sciences (e.g. physics, chemistry, biology) (Ponelis, 2015) with a focus on statistics (Corbetta, 2013). Therefore, the paradigm of positivism uses theoretical groundwork as the main investigative tool. Positivism often believes that truth is researchable and objective, so its epistemology includes a deductive design of test (Lincoln and Guba, 2011) .

In the paradigm of positivism, there are two versions: original and post positivism (Corbetta, 2013). During the mid-nineteenth century, researchers considered positivism to be the mode in which reality is the primary subject for researchers who follow original theory (Bell, 2017). Researchers who support original positivism should be impartial in terms of the data. In addition, in a value-free approach, analysis that adopts original positivism is conducted (Gray, 2018). In this paradigm, researchers can compile data using existing theory to develop the hypotheses that lead to further development (Saunders et al., 2009). In comparison, the assumption of social truth is more significant in post-positivism. In post-positivism truth continues to be the objective but it is fallible in some way (Corbetta, 2013). Original positivism, thus, appears to be the conventional approach to science, whereas post-positivism is a new approach that perceives a degree of ambiguity (Bell, 2017), Consequently, information is interpreted in the context of probabilistic legislation (Donatella Della Porta, 2008). These methodologies are motivated by a distinction between the researcher and the entity being observed but qualitative approaches may criticise and evaluate hypotheses (Corbetta, 2013).

3.1.2 Interpretivism paradigm

The interpretivist paradigm is characterised as a philosophical stance that uses naturalistic methods and concentrates on context-specific settings on a holistic interpretation of human

experiences (Ponelis, 2015). Naturalistic approaches include the study without intervention of the actions of subjects in their natural environments. The objective and the subjective are interdependent in this paradigm (Bell, 2017). In addition, there is no true truth because there are many realities that differ between individuals, groups and cultures in form and content (Corbetta, 2013). In other words, this means that the universe can be examined and clarified but not in terms of numbers (Bell, 2017). This perspective conveys the general belief that life and the universe consist of multiple aspects of truth that different people recognise differently (Stiles, 2003). The interpretive research approach focuses on significance, meaning and intent (Corbetta, 2013). Due to the fact that this model looks at the world from a stance that could prove beneficial from several viewpoints and, therefore, its interpretation should be from multiple perspectives (Alharahsheh and Pius, 2020). Consequently, if the study goal is to understand the importance that subjects assign to their own behaviour, the research methodology will be qualitative and subjective (Baškarada and Koronios, 2018). Depending on the relationship between subjects and researchers, the discovery will vary from case to case (Baškarada and Koronios, 2018). Therefore, it is very important for researchers to consider the societal world of the reviewed subjects from their point of view (Corbetta, 2013; Saunders et al., 2009).

3.1.3 Pragmatism paradigm

Research paradigms help to direct the research process. However, in some cases, because of the various characteristic and multi-dimensional categories of a particular study, it may be impractical to choose a single model for use in the entire research. Paradigms help direct analysis, but they are rather impractical in certain cases when selecting a single role between positivism, post positivism and interpretivism (Corbetta, 2013). For this reason, when seeking to answer specific practical questions, researchers may opt for pragmatism (Baškarada and Koronios, 2018). Pragmatists claim that the research issue is the most critical aspect of a research theory (Baškarada and Koronios, 2018). A realistic approach can be applied with this research paradigm, combining diverse views to help collect and analyse data (Saunders et al., 2009). Other paradigms consider a phenomenon as a compilation of facts, whereas the paradigm of pragmatism offers meaningful insight in practice (Johnson et al.,2007). In the pragmatist model, researchers can manipulate tasks in their research environment. The essence of knowledge and its practical dimension are well suited to this research (Blosch, 2001). When a system is developed on a realistic basis, the relationship between awareness, meaning and practice is underlined. Understanding this connection thus provides both practitioners and researchers with a workable strategy to create a knowledge-based organisation (Baškarada and Koronios, 2018).

3.2 Research approach

Most of the work in this thesis primarily follows the positivist paradigm but with a slight hybrid approach in that the current research also considers qualitative (interpretivism) views where appropriate. Thus, the theoretical foundation of this thesis is in a hybrid of interpretivism and positivism. A hybrid approach was required. This is because eliciting the current issues with access management for digital twins in the built environment did not only require quantitative analysis, but also some qualitative analysis of survey data.

In terms of research philosophy, the current study has followed the deductive reasoning approach, whereby theories and hypotheses are established first and then tested to validate or reject them. In scientific studies, this is a common strategy (Alam, Halder and Pinto, 2021). As a result, tests, as the foundation for validation, necessitate rigour, control and a systematic methodology and positivism studies usually adopt the deductive approach (Alam, Halder and Pinto, 2021).

Thus, the following hypothesis and research questions have been proposed:

The introduction of a built-environment access management work adapted to new technological advances will ensure the security and interoperability of built environment digital twins with existing ICT systems in common use today.

The research questions are as follows:

RQ1: *How suitable are the current IoT and CPS security systems for providing access management for digital twins in the context of smart buildings and districts?*

RQ2: *What are the current obstacles to tackling access management threats to the built environment CPSs?*

RQ3: *What are the key requirements for a semantically specified access management framework suitable for the built environment?*

RQ4: *Can the current security processes employed by CPS and digital twins be improved to address the access management requirements of digital twins in the context of the built environment?*

The current study's focus on decision-making includes both social processes and elements of nature, as well as conceptual and methodological components. Thus, it is necessary to apply a participative approach. As a result, this necessitates the employment of a participatory action

research technique which is the most common type of study in information systems (Di Mascio *et al.*, 2019). Participatory action research is a type of action research that involves practitioners as both respondents and co-researchers. This participatory strategy is implemented by means of direct engagement with stakeholders and their inclusion in the loop as well as collaboration with specialists and the use of surveys.

Thus, there are two primary forms of research used in this thesis: explanatory and descriptive (Baškarada and Koronios, 2018). Explanatory research has been shown to be useful when investigating problems with a degree of uncertainty in their organisation but it has to be tested using different forms of expertise; for example, a researcher's ability to observe and then recognise certain issues (Ghauri, Grønhaug and Strange, 2020). However, if circumstances require specific levels of life to be examined and the achievement of ground-breaking conclusions about an emerging phenomenon from a different viewpoint (Saunders et al., 2009). Descriptive research can be very helpful at providing a straightforward description of such phenomena, so this form of research allows systematic to resolve issues (Saunders et al., 2009). In addition, descriptive analysis discusses structurally ordered concerns very well (Ghauri, Grønhaug and Strange, 2020).

This research falls within the explanatory and descriptive categories of research because it aims to explore the ICT and collaborative practices of BIM-based projects and the potential of digitals twins to leverage access management, access control and single sign on solutions.

Once a paradigm, philosophy and category of research is decided upon the researcher must then decide on a selection of research methods. In general there are three approaches: quantitative approach (i.e. positivist research paradigm), qualitative approach (i.e. interpretative research paradigm) and hybrid approach (i.e. mixed quantitative and qualitative approach) (Fellows and Liu, 2015; Saunders, Lewis and Thornhill, 2019; Panas and Pantouvakis, 2010; Ponelis, 2015).

It is possible to track the choice and selection of a quantitative method back to the late 20th century (Baškarada and Koronios, 2018). According to Polit and Beck (2013), the quantitative approach can be defined as an investigation of phenomena that provides reliable measurement and quantitative action, often requiring a rigorous and controlled design. In addition, Baškarada and Koronios (2018) notes that quantitative analysis deductively involves testing assumptions. The quantitative approach is connected to positivism and aims to collect factual evidence in order to research the relationships between particulars and how these facts and relationships comply with hypotheses and the outcomes of previous studies (Fellows and Liu, 2015). Quantitative data are gathered in a quantified (numeric) form that, if necessary,

can be calculated and analysed using statistical methods (Polit and Beck, 2013). Results and assumptions are drawn from a review of results in light of the empirical literature and theory (Richard Fellows and Liu, 2015).

On the other hand, the qualitative approach aims to obtain perspectives and collect the opinions of people (Fellows and Liu, 2015). This technique is widely used in interpretivist research. According to Polit and Beck (2013), qualitative analysis is the study of phenomena (generally breadth and holistic fashion) through the selection of rich narrative materials utilising a versatile research design and, as a consequence, data can be unstructured (raw form) but completely detailed and rich in content and scope where people's beliefs, understandings, perceptions and opinions can be examined (Fellows and Liu, 2015). This makes data analysis much harder than when applying a quantitative approach, involving a great deal of filtering, sorting and labelling to make the information suitable for reporting (Fellows and Liu, 2015). Because qualitative research offers a way to investigate and interpret the importance of a social or human issue for individuals or groups (Baškarada and Koronios, 2018), the following methods are also usually used in qualitative research: interviews, evaluation, record review and case studies (Cooper and Schindler, 2014).

Several researchers agree that when conducting rigorous research, a mixed-methods (triangulation) approach may be valuable (Ponelis, 2015; Fellows and Liu, 2015). Triangulation involves using several testing techniques within the same research inquiry for different purposes (Saunders, Lewis and Thornhill, 2019). Thus, triangulation employs more than one research system or method of data collection within the same analysis (Bell, 2017). The use of multiple methods minimises or eradicates the drawbacks of each individual approach while at the same time realising many of the benefits of using both together (Fellows and Liu, 2015). In different fields of study (e.g. management, science and engineering), the mixed-method approach is increasingly chosen as the primary research approach (Peng and Annansingh, 2015; Azorín and Cameron, 2010). The advancement of technological progress in the field of computer and engineering research includes not only technical aspects but also social, legal and financial viewpoints (Lethbridge, Sim and Singer, 2005).

The timing of data collection in the mixed method approach might be in the form of a sequential, concurrent or transformative operation (Baškarada and Koronios, 2018). Quantitative and qualitative data are processed in a sequential operation at the same time. Either the compilation of qualitative data begins, followed by quantitative data or vice versa. The researcher obtains both quantitative and qualitative data at the same time and in the same form and analysis gives equal priority to all types of data. In contrast, in the sequential form, priority is given to the data type collected. This sort of form gives all types of data equal priority.

Therefore, when investigating the research subject, triangulation is very effective, following many alterative paradigms or techniques (Fellows and Liu, 2015).

Furthermore, ethical principles direct a study from its conceptual phases, from fieldwork to final interpretation, and reviewing the findings in part of every research project undertaken (Miura *et al.*, 2021). According to Fellows and Liu (2015), when conducting a study there are many ethical considerations such as accuracy, honesty and the confidentiality of the data collected; the participants should be told about the aims of the research, participation should be voluntary, and privacy should be preserved. to protect personal information about the user. Additionally, we have expanded this to describe how confidentiality should be preserved to ensure confidential information stored within digital twins is protected. These guidelines, along with ethical and privacy law training, have ensured that the principles required in the field of computer science are met.

This section provides a thorough description of the selected methodology to answer the stated research questions. In addition, there is a comprehensive description of not only the approach applied but also the philosophical stance, thereby providing insight into the way in which knowledge has been acquired. The current chapter introduces the mixed method approach that has been applied as well as participatory action research and a description of the associated research undertakings, the use of a survey to amass the necessary data and the selected case studies. Research into access management approaches for digital twin technology is a new area of study within the built environment domain. Initially a literature review driven approach was considered.

However, this found that literature in this area is still relatively sparse. Then a survey driven approach was considered, to examine industry views, but this found that experts in the built environment have differing perspectives and understandings of this domain.

These obstacles were only overcome by using a systematic multi-phase research approach (literature review, industry survey, eliciting obstacles and defining the access management framework, ontology development and validation). The current research involves five phases, and these are described in more detail below.

Phase 1: This phase involves conducting a literature review, performing initial research into current solutions, eliciting an understanding of how suitable the current IoT and for CPS security systems are in terms of addressing the access management threats facing digital twins in the context of smart buildings and district. This section will also define and decide upon the necessary research tools for this study. This phase also involves defining the possible testing methods to be utilised during the investigation.

Phase 2: This phase involves the collection of primary data for the development of digital twin-based CPS built environment solutions. This phase involves the case studies and surveying the reference zones of built environment experts. From this a set of obstacles are elicitied.

Phase 3: The obstacles identified in phases 1 and 2 are then analysed and evaluated. Based on this analysis, this phase defines the built environment cyber-security framework required to resolve the previously elicited obstacles.

Phase 4: This phase entails the process of ontology development to produce the semantic conceptualisation needed to deliver the cyber-security framework. An ontology provides a useful methodology for formalizing the semantics and relationships that must be formed between access management and built environment concepts.

More specifically, ontologies define an explicit domain-specific semantic schema that can explain real-world concepts and relationships. This is required in the access management domain as there is already multiple heterogeneous sets of concepts (i.e., IoT concepts, BIM concepts etc…) that must be aligned with access management concepts. Thus, taking an ontology driven approach enhances interoperability because information is treated in terms of its formalised semantics.

Phase 5: This phase validates the final access management framework using a new case study, validating the semantic representation against the compliance questions previously elicited.

3.3 Phase 1: Literature review

This phase entails conducting a literature review (relating to BIM, cyber-physical systems and their driving technologies, semantic web technologies, smart buildings, digital twins, cybersecurity), conducting research on existing solutions, eliciting significant impediments to be addressed by the research, and identifying and selecting the research tools required for the current project. During this phase, the possible testing methodologies to be used during the study are defined.

The thorough literature assessment described in Chapter 2 constitutes a research strategy in and of itself. It enables the formation of theoretical underpinnings and an overarching depiction of the topic. Many knowledge resources must be evaluated and critically compared. Furthermore, given the integrative and design-oriented nature of the answer sought, a review of current technologies is critical because the research focuses on refining existing methods

rather than developing new ones. This phase of the research will answer the first research question.

3.4 Phase 2: Industry survey

This research will utilise the survey instrument to help gather information from experts on the formulation of key performance indicators for cybersecurity. As the objective of this research is to develop a framework that meets the requirements of the built environment industry, an extensive and quantitative/ qualitative method is preferred. However, due to the complexities of the topic of cybersecurity, different qualitative questions will be required to better capture a specific perspective.

3.4.1 The Survey Research Instrument

A survey is a technique that tries to collect data through the responses to questionnaires or interviews. A survey might be quantitative or qualitative, positivist or interpretivist, depending on its structural scope. Survey are a pre-defined collection of questions and items prepared to respond to the questions in a pre-determined order, providing the researcher with information that can be evaluated and interpreted (Ponelis, 2015). Surveys are sometimes sent by post to a group of individuals who are invited to complete and return it to the researcher, or they are often created using web-based survey tools. They are often correlated with the survey study technique (Cooper and Schindler, 2014). In other study methods such as interviews, case studies, action research or design and development, surveys may be used (Ponelis, 2015). Surveys are widely used because they offers an easy way to gather data from a broad number of respondents in geographically diverse locations (Lethbridge, Sim and Singer, 2005). In a structured and systematic way, surveys collect the same kind of data from a large number of people (Fellows and Liu, 2015). Interpretive and critical analysis can be applied (Çelik *et al.*, 2018). A popular use of a survey in computing is in a software system's user assessment, although it should be said that such surveys seem to have been labelled at the end of system development because they tend to be badly planned and implemented (Ponelis, 2015).

Ponelis (2015) suggests that the use of surveys in research offers many advantages including: (a) to obtain data from a large number of individuals; (b) to obtain reasonably brief and uncontroversial information from individuals; (c) to obtain uniform data by posing similar questions to each respondent; (d) expecting participants to be able to read and comprehend the questions and potential answers; (e) time and cost efficiency, particularly when web-based questionnaires are used; (f) questionnaire results can typically be quantified quickly and easily by the researcher or by using a descriptive software package; (g) it is possible to interpret the

findings in a more scientific and analytical manner than when applying alternative types of research; (h) quantified studies may be used to directly compare other studies and may be used to calculate changes; (j) positivists assume that to construct new ideas and/or test current hypotheses, quantitative evidence should be used.

On the other hand, Lethbridge, Sim and Singer (2005) and Karl Popper (2010) have identified the following disadvantages associated with surveys: (a) unclear and badly expressed questions may be problematic, especially when the researcher is not there to explain; (b) the chosen participants may not have time to fully complete the questionnaire; (c) it is claimed that such knowledge derived from thoughts, actions, feelings, etc. may be difficult to understand; (d) it lacks authenticity and is hard to tell how truthful a respondent is; (e) respondents may perceive each question differently, and then respond on the basis of their own interpretation of that question, so the degree of subjectivity goes unrecognised.

3.4.2 Implementation of Surveys in this Research

The survey utilised in this project will hosted by Jisc online survey (Online surveys, 2020) which is a UK-based organisation whose function is to help promote higher education and those organisations that undertake research. It offers network and IT services, digital tools, suitable advice and advisory services for procurement while at the same time exploring and implementing new information technology and working methods. Surveys are distributed to built environment experts and their answers are gathered for study and interpretation. This phase of the research will help to answer the second research question.

3.5 Phase 3: Eliciting obstacles and defining the access management framework

This phase will determine obstacles to the adoption of access management for digital twins/CPS in the built environment (from phase 1 and 2) and these are then analysed and evaluated. Based on this analysis, this phase also defines the key constituents of the built environment cyber-security framework required to resolve the previously elicited obstacles. This phase of the research will answer the second research question.

3.6 Phase 4: Ontology development

This phase of the research will focus on the definition of the semantic cyber security framework. Specifically, the ontology design.

The earliest part of ontology creation is perhaps the most crucial. It should be approached with caution because any errors may result in the design of the ontology being either structurally or conceptually lacking. To avoid such misunderstandings, the NeOn approach

encourages the use of the Ontology Requirement Specification (ORS), a 'METHONTOLOGY' (Tapia-Leon *et al.*, 2019). The goal of the ORS is to clarify the domain needs and aspects that the ontology must address. It consists of three distinct steps: (1) identifying the future ontology's goal; (2) identifying the ontology's intended uses and customers; and (3) identifying the set of requirements that the ontology must meet (Kibria *et al.*, 2017). Furthermore, the scope of the ontology and the domain targeted must be defined. This stage of the research will answer the third research question.

The use of competency questions can help define the requirements quickly and effectively. For ontological growth, competency questions are widely employed (Roberto and Davis, 2020; Tapia-Leon *et al.*, 2019; Kibria *et al.*, 2017; Neto, Jorge and Nascimento, 2021). They are simply queries that the developed ontology should be able to respond to. The questions are first defined in an informal manner using common language. This helps to define the ontology's scope as well as to understand recurring terms. Once the author has a deeper understanding of the topic, formal questions are constructed to extract precise terminology, attributes, relationships and axioms. The question must be organised in a logical manner with many levels of abstraction ranging from simple to sophisticated (Neto, Jorge and Nascimento, 2021). As a result, requirements progress from a vague and ambiguous definition to a more precise and valuable system.

3.6.1 Semantic modelling

The method of developing an ontology is depicted in Figure 3.1. The approach is more complicated and is highly dependent on the domain in question as well as the degree to which current ontologies are reused.

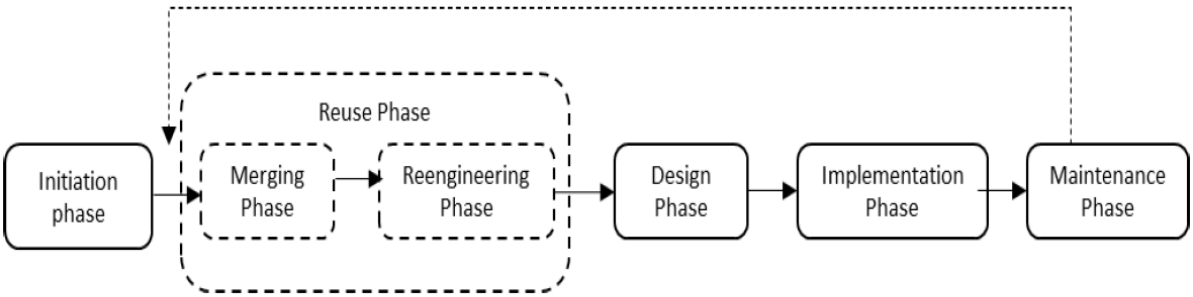


Figure 3.1 *NeON methodology* (Suárez-Figueroa, Gómez-Pérez and Fernández-López, 2015)

The NeOn project has proposed nine scenarios that could be used to create an ontology. Figure 3.2 depicts all nine scenarios identified by the NeOn technique as well as their interrelationships. The utilisation of knowledge resources, particularly existing ontologies, differs significantly between the various scenarios. The developer has the option of creating

direct alignments, re-engineering or reusing the current design patterns, depending on how well the old ontologies meet the new ontology needs. Because the first scenario includes the basic activity of ontological growth, it must be coupled with a second scenario. These examples emphasise the need to reuse resources, particularly ontology, thereby indicating the field's conceptual focus on developing extensive and interconnected knowledge and understanding.

As part of the current study, the ontology underpinning the semantically defined access management framework will be developed utilising the NeON methodology, making the maximum possible use of the existing ontological and non-ontological resources. This is necessary to ensure that the developed ontology is both applicable to the smart cities/digital twin domain and suitable for integration with other state-of-the-art developments.

As previously mentioned, there are two types of knowledge resources: non-ontological and ontological resources. To derive a sufficiently rich ontology and, given there is an absence of ontological resources in the smart city/digital twin domains, four case studies will be mined for

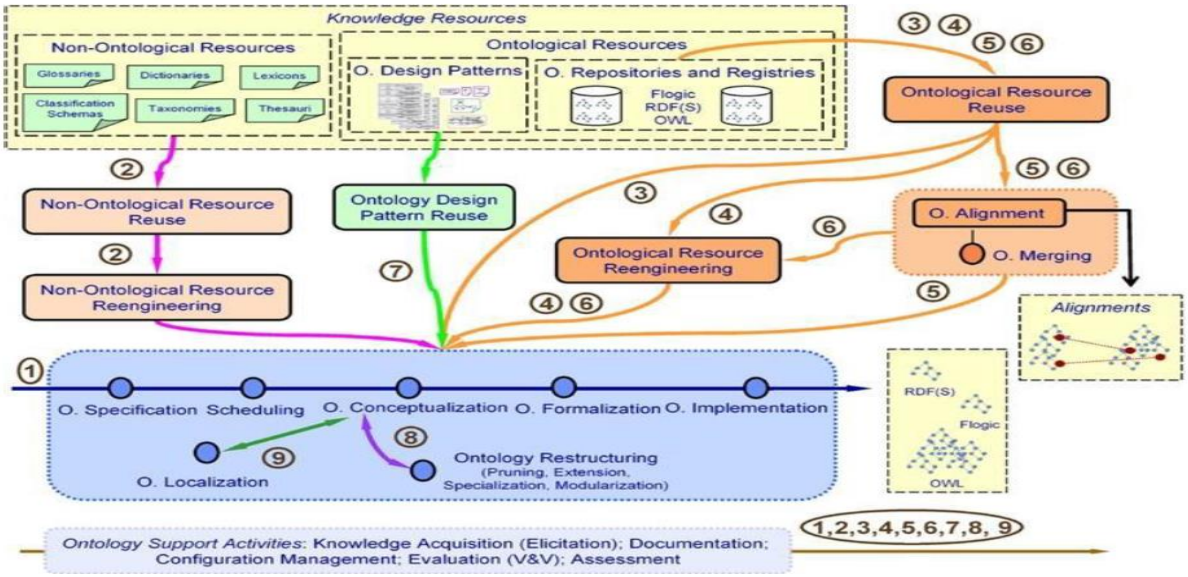


Figure 3.2 *NeON scenario representation* (Suárez-Figueroa, Gómez-Pérez and Fernández-López, 2015)

non-ontological resources. These use cases will be formed by extracting domain information from resources such as glossaries, taxonomies and thesauri. Based on this, explicit UML models will be constructed along with competency questions to validate the semantisation of these use cases. These techniques are described in the following subsections.

In addition to this mining of case studies, the ontological resources that are available in the domain will be reviewed and incorporated.

In summary, the ontology development methodology undertaken in this work is as follows:

- Use the NeOn approach to the Ontology Requirement Specification (ORS).
- Define the overall ontology competency questions.
- Acquire and formalise into UML the non-ontological resources mined from case studies and define any use case-specific competency questions.
- Analyse the existing relevant ontological resources.
- Engineer non-ontological resources into ontological resources.
- Align ontological resources.

3.6.2 Case studies

As previously stated, this work will make use of case studies. Case studies are utilised as an instrument to intensively explain and examine a particular person or community in order to discuss and appreciate complex problems within their real life context (Zainal, 2007). Particularly when a holistic, in-depth inquiry is required, it offers an effective research method (Zainal, 2007). Case studies have been described by Rashid *et al.* (2019) as an empirical investigation into a contemporary phenomenon (e.g., a case), particularly when the borders between phenomena and situations are not clear within the real-world situation. As reported by Rashid *et al.* (2019), there are three key reasons for using a case study as a form of research: (a) explanatory or descriptive questions can be included in the research; (b) the case study method supports other research methods in combination data in normal configurations by highlighting the analysis within a phenomenon of its real-world background; (c) it is suitable when a researcher needs to perform an assessment analysis.

Rashid et al. (2019) stated that the use of case studies in research offers many advantages including: (a) simplifying complicated concepts by introducing the researcher to circumstances in real life that can often be difficult; (b) helping to provide the researcher with new information by exploring particular topics; (c) helping to improve critical thought, communication and tolerance for difficult opinions about the same problem; (d) providing the researcher with a chance to innovate; (e) the possibility to involve biases in the collection and analysis of the data.

On the other hand, Rashid *et al.* (2019) also recognise that there are many disadvantages associated with case studies including: (a) it may be difficult to obtain a suitable case study to fit all subjects; (b) case studies involve the observation of the study and the interpretation of individuals, so that there is a possibility that the individual reporting the case study may present the case study in one way, whilst other aspects are entirely missing; (c) in general, case studies are more time-consuming that alternative data collection instruments; (d) there is no

correct answer owing to the fact that different people will have different perceptions of the same thing; and (e) it is influenced by the maturity level of the participants.

Many previous researchers have opted for a case study approach. For instance, Barlish (2011) used case studies to develop a BIM benefit measurement scale by empirically measuring data from non-BIM and BIM projects and evaluating whether the use of BIM in construction projects can be beneficial.

3.6.3 UML modelling

As described previously, due to the paucity of empirical studies relating to DTs and the IoT in the built environment, especially about access management, the case studies in the current study will be modelled using UML to formally document them (see Appendix D).

Modelling is a part of the method of developing software systems prior to the commencement of programming (OMG, 2017). Modelling is now an important component of significant software projects and is very useful for small and medium sized projects. In software development, a model plays a role in the drafting of software plans by software developers. Developers can ensure that their software system's business functionality is complete and accurate and that end-user requirements are met with the use of a model. Therefore, prior to coding, a model provides the specifications for security, scalability, robustness, extensibility, and other features. This helps to prevent costly mistakes and complicated modifications during the implementation stage (OMG, 2017). There are several modelling languages according to List and Korherr (2006) but the most dominant in modelling are the following: Unified Modelling Language (UML) (OMG, 2017), Business Process Description Metamodel (BPDM) (Aagesen and Krogstie, 2010), and Business Process Modelling Notation (BPMN) (Aagesen and Krogstie, 2010).

Several studies indicate that large software projects are highly likely to fail because most of these projects have struggled to satisfy all of their demands within the available timeframe and budget (Lehtinen *et al.*, 2014). However, modelling and visualising the structure of the software project and testing it before coding against its specifications helps to reduce the risk of failure and helps to progress the project by allowing higher abstraction levels to be worked on (Voightmann, 2004). This can be achieved by hiding smaller details, focusing on the larger picture or emphasising the prototype's special features (OMG, 2017).

In built environment science, there are several researchers who have used BPMN and UML. UML has been adopted as the standard modelling language for software system modelling (Bendraou *et al.*, 2010). It helps to describe, envision, and document models of software

systems in a manner that satisfies all system specifications, involving internal and external design. It is important to model the software system architecture. However, it can also be used to model other non-software systems for business modelling (OMG, 2017). Although some software and company processes are identical, there is some variability; business systems have some principles that are not intended to be implemented in a software program (e.g., production machines, people, rules and goals). However, UML was originally designed to define a software system's features, it needs to be expanded to explain and cover more process orientated aspects, i.e. operations, priorities, resources and business system rules (Eriksson, 2001). Using UML modelling enables the researcher view a detailed view of an application, offering a representation of the relationship between the application to other applications. In addition, the researcher can concentrate on different aspects of the application, such as business operations or the observation of its business principles. There are almost thirteen forms of UML diagrams according to OMG (2017). These are split into three types:

- **Structure diagrams** involve class diagram, object diagram, composite structure diagram, component diagram, package diagram, and deployment diagram.
- **Behaviour diagrams** are used during the collection of requirements in certain methodologies and include the action diagram and state machine diagram.
- **Interaction diagrams** include the sequence diagram, the contact diagram, the pacing diagram, and the interaction summary diagram which are derived from the general behaviour diagram.

In this research UML is used to explain in greater detail the internal design and functionality of the case studies. The UML use case diagram can model many use scenarios. In addition, the class diagram is used to define the internal IoT structure.

3.6.4 Competency questions

Competency questions offer a helpful way to establish the complexity of an ontology because they list a collection of questions that an ontology-based knowledge should be able to address (Hippolyte et al., 2018; Vajpayee and Ramachandran, 2019; Tapia-Leon et al., 2019; Tarasov, Seigerroth and Sandkuhl, 2019; Vajpayee and Ramachandran, 2019). This thesis will use competency questions to aid in the formal ontology requirement specification.

3.7 Phase 5: Verification & Validation

This phase will validate the final access management framework. Firstly, this phase verifies semantic representation against the competency questions previously elicited. Secondly, its

functionality is validated on a new case study. This case study will then be formally modelled using UML to explicitly document its requirements. Then the semantic access management framework will be initialised for this case study and tested. This will include testing its compatibility with the required concepts for the built environment such as SSO. This phase of the research will answer the fourth research question.

3.8 Summary

This section has defined the methodology for this research. A methodology has been selected that is sufficiently versatile to compromise workable approaches given the built environment consists of dynamic social-organisational interactions It has factored in an understanding ICT and IoT practice during a construction project.

Thus, a hybrid approach has been selected. This is underpinned by the theory of pragmatism which maintains that analysis often takes place in social and other contexts. This chapter has also summarised the following: the research theory, research questions, research design, research methods and research strategies. It is possible to summarise the selected method as follows: (a) research paradigm: positivism, interpretivism and pragmatism; (b) research approach: phase 1, phase 2, phase 3, phase 4, phase 5. Table 3.1 summarises the overall methodology applied in the current Ph.D. study. This is shown in more detail in Table 3.1

Table 3.1 Summary of the methodological

The adopted approach	
Research paradigm	Positivism, Interpretive and pragmatic
Research approach	Inductive
Strategies	Analysis and modelling process strategies
Type of research	Descriptive and explanatory
Research methods	Mixed methodology (quantitative, qualitative), software development
Techniques and procedures	Data collection, analysis and modelling using UML, ontology
Software development	Jisc online survey, visual programming, protégé

Chapter 4: Survey of access management for digital twins in the built environment

This chapter presents the industry survey that has been conducted the aim of conducting this survey was to answer the second research question**:** *What are the current obstacles to tackling access management threats to the built environment CPSs?* This chapter describes how this work has been conducted.

The survey contained twenty-four multiple-choice and open questions in sections coverings: (a) understanding of the adoption of the cyber-physical system regarding the built environment; (b) understanding the adoption of digital twins in the built environment; (c) determining obstacles to the adoption of access management for digital twins/CPS in the built environment.

4.1 Designing the built environment survey

The survey was distributed via the European Construction, built environment and energy efficient building Technology Platform (ECTP), social media and individual contacts with experts. The survey comprised 24 questions and was targeted at built environment and industry professionals with experience of adopting access management for digital twins/CPS in the built environment.

Because consultation necessitates extensive knowledge across multiple domains, finding suitable experts is critical to the study's relevance. Furthermore, to prevent bias, expert selection must adhere to specific requirements. Before selecting experts, the researcher should acknowledge certain criteria such as gender, work experience, education, job opportunities, or designation. To reduce bias and discussion issues, it is recommended to consult experts with various areas of knowledge in various locations (Fugar and Adinyira, 2019) .

In terms of panel size, there is no evidence to support an optimal panel size. However, it is frequently advised to survey between 20 and 50 experts in various areas of expertise (Fugar and Adinyira, 2019; Hordijk *et al.*, 2019).

The experts surveyed were chosen based on their expertise in a variety of fields. Research articles relating to urban cities, ICTs, the IoT, digital twins, and cybersecurity assessment schemes, among other topics, were reviewed and researchers were contacted when the content was found to be useful for the survey. In total, 33 of the 150 experts contacted indicated that they would be happy to participate. The experts were all engaged in research

at reputable universities or companies, and the survey was distributed via the ECTP, due to its membership basis possessing a high number of technologically relevant organisation. To ensure correct and valid responses the survey advised that experts about the particular emphasis and purpose of the study as recommended (Hordijk *et al.*, 2019).

The industry survey itself (see Appendix A) comprised twenty-four multiple-choice and open questions across various categories. First, the survey focused on gathering demographic information such as the respondents' work experience, roles in their organisations, and type of organisation they work for. Secondly, the survey sought more specific information about the current use of cyber physical systems and digital twins in their work in the built environment. It was then important to establish the advantages and barriers they experienced when using digital twins during projects. The respondents were then asked about any issues they have with managing threats in digital twin/cyber physical systems and the types of access management that they have in their organisations to understand and determine the behaviour that affects IoT/digital twin usage. Subsequently, they were asked which criteria are important to enhance adoption of digital twins/cyber physical systems and cybersecurity in the built environment.

4.2 Built environment experts' responses

The survey was distributed widely (as described previously) and 33 respondents completed the survey (all of the responses were valid responses).

Table 4.1 Built environment experts' responses

Category	**Experts' responses**
Participants' work experience in the built environment	36.4% of the participants have 0-10 years work experience 39.4% of the participants have 10-20 years work experience 18.2% of the participants have 20-30 years work experience 6.1% of the participants have more than 30 years work experience

Participants' roles in their organisations	12.1% structural engineers 18.2% architectural engineers 9.1% BIM managers 21.2% developers 39.4% of the participants gave other responses: • 7.69% Director, • 7.69% Electrical engineering, • 7.69% Research and development engineer, • 7.69% Urban planner, • 7.69% Founder urban design firm, • 7.69% Postdoctoral researcher, • 7.69% Innovation manager, • 7.69% Researcher, • 7.69% Professor: education & research, • 7.69% University of technology, • 7.69% Head of department, • 15.38% R&D project management.
Participants' organisation type	3% structural design 15.2% strategic planning 12.1% multidisciplinary engineering consultancy 15.2% multidisciplinary (design, construction) 54.5% of the participants gave other responses: • 22.22% Research institute, • 16.66% Extraction company, • 11.11% IT company, • 11.11% University, • 5.55% Real estate, • 5.55% ICT, • 5.55% Urban design, • 5.55% ROT, • 5.55% Research and development centre,

	• 5.55% Research and teaching, • 5.55% Public client.
Participants' organisation's use of Cyber-Physical/IOT Systems	51.5% don't use the cyber-physical/IOT systems 48.5% use the cyber-physical/IOT systems
Participants' problems when using Cyber-Physical/IOT Systems	63.2% data protection and data security 47.4% data exchanging 31.6% lack of benefit quantification 10.5% of the participants mentioned other problems in their organisations
Participants' organisations will use the Cyber-Physical/IOT Systems in future	30.3% of the participants will use it in the short term 33.3% will use it in the long term 33.3% will not use this system in their organisations 3% gave another response
Participants' organisations use of digital twins	51.5% use digital twins 48.5% don't use digital twins
Participants' projects deploy digital twins	39.4% deployed digital twins in projects 60.6% don't deploy digital twins in any project
Barriers to using digital twins	41.7% training skill 41.7% limited access to data 50% cost 41.7% applicable technology 16.7% of the participants mentioned other barriers with using digital twins
Existence of a cybersecurity team to manage and design digital twins/CPS	42.9% have a cybersecurity team in their organisation

	57.1% don’t have a cybersecurity team in their organisation
Managing threats associated with digital twins/CPS	41.7% lack of export in security management 50% lack of technology 25% cost 8.3% of the participants referred to other issues
Type of authentication in participants' organisations	78.6% log in (username and password) 7.1% biometric (iris scans, fingerprint scans and voice recognition) 14.3% of the participants use other types of authentication
Existence of controls to classify data in terms of criticality and sensitivity	64.3% have controls to classify sensitive or critical data 53.7% don’t have controls to classify sensitive or critical data
Type of controls used to classify data	77.8% availability as a type of data control 55.6% confidentiality as a type of data control 44.4% integrity as a type of data control
Existence of tools and processes to find and prevent sensitive data from leaving the digital twins/CPS	38.5% have tools or processes to find out and prevent sensitive data from leaving the DT/SPSs 61.5% don’t have tools or processes to find out and prevent sensitive data from leaving the digital twins/CPSs
Existence of monitoring of digital twins/CPS to detect anomalous activities	42.9% can monitor digital twins/CPSs to detect anomalous activities 57.1% can’t monitor digital twins/CPSs to detect anomalous activities

Existence of plans to use digital twins/CPS in participants' organisation in the future	54.5% have plans to use digital twins/CPSs in future 45.5 % have no plans to use digital twins/CPSs in future
Use of digital twin technology in participants' organisation	39.4% use digital twins technology in urban design development 48.5% use digital twins technology in data analysis 57.6% use digital twins technology in building operations 36.4% use digital twins technology in control access
Training skills to enhance adoption of digital twins/CPSs in the built environment	46.9% extremely important 43.8% very important 9.4% somewhat important
Relevant technology to enhance adoption of digital twins/CPSs in the built environment	25% extremely important 50% very important 25% somewhat important
Developing a smart application architecture to enhance adoption of digital twins/CPSs in the built environment	35.5% extremely important 32.3% very important 29% somewhat important 3.2% not at all important
Smart grid to enhance adoption of digital twins/CPSs in the built environment	9.4% extremely important 50% very important 34.4% somewhat important 6.3% not at all important
Expand BIM specifications to become IoT compliant to enhance adoption of digital twins/CPSs in the built environment	28.1% extremely important 46.9% very important 18.8% somewhat important

	6.3% not at all important
Training skill to enhance adoption of cybersecurity for digital twins/CPSs in the built environment	45.5% extremely important 42.4% very important 12.1% somewhat important
Relevant technology to enhance adoption of cybersecurity for digital twins/CPSs in the built environment	32.3% extremely important 45.2% very important 22.6% somewhat important
Developing a smart application architecture to enhance adoption of cybersecurity for digital twins/CPSs in the built environment	45.2% extremely important 32.3% very important 22.6% somewhat important
Smart grid security to enhance adoption of cybersecurity for digital twins/CPSs in the built environment	43.8% extremely important 34.4% very important 18.8% somewhat important 3.1% not at all important
Expand BIM specifications to become IoT compliant to enhance adoption of cybersecurity for digital twins/CPSs in the built environment	29% extremely important 35.5% very important 25.8% somewhat important 9.7% not at all important

Text has been added to the thesis to acknowledge the potential impact from having this sub-group in the findings. However, overall, this is a minority of responses (~20%) - and that while it indicates some doubt the vast majority of the respondents, and the evidence from the literature support the conclusions of this work. Thus, this element of doubt, while important to does did not invalidate the rest of the work.

4.3 Participants' comments

The participants gave different responses to a range of issues including problems with using cyber-physical/IOT systems, the advantages, barriers, type of access to data, the type of authentication, types of tools and processes to find out and prevent sensitive data and plans to use digital twins/CPS in their organisations in future. The open questions in the survey are presented in Table 4.2.

Table 4.2 Participants' comments

Participants' problems when using cyber-physical/IOT systems:
"Standardisation - accessing control over different platforms from different providers in a uniform way has not been handled well so far." *"No standard data format."*
The advantages of using digital twins during the project:
"Transforming cities into smart cities will support the IoT, especially in the design phase." *"Facilitate the design."* *"Realtime monitoring and performance analysis."* *"Reliable representation of the physical system."* *"Read sensors easily and implementing tools for facility management."* *"Key performance indicators for urban districts and entire cities."* *"The required input data for the many different kinds of simulations (energy consumption and production, traffic flows, noise dispersion, air quality) can directly be derived from the digital twin."* *"We can clone the digital twin and create scenarios by modifying the semantic 3D city model and can immediately run the same stack of computations and simulations on the modified digital twin for impact assessment of planned actions."* *"Better communication between different project parties."* *"Real time assessment of structural behaviour."*
Barriers to using a digital twin:
"Keeping the digital twin for entire urban districts (or even cities) up-to-date is very difficult."

"Assessing data integrity; the data that belong to digital urban twins is not in the hands of a single owner (like the manufacturer of a machine/device) but spread over many stakeholders."
Type of access to data in the digital twins/cyber physical systems:
“Dedicated team.” *“Researchers and project leaders.”* *“We use an open format: Node Red.”* *“BACS network.”*
Type of authentication in participants' organisations:
“*Two factor authentication.”* *“Kerberos and Keycloak technologies.”*
Types of tools and processes to find out and prevent sensitive data from leaving the digital twins/CPSs:
“Open source for IoT platform, gateway and physical sensors.” *“Architectural programs.”* *“Local.”* *“Oauth2, SAML2, OpenID Connect*.”
Plans to use the digital twins/cyber physical systems in participants' organisation in the future:
“Involving all stakeholders in the urban design process to get the most out of information communication technology.” *“Integrate into IoT devices.”* *“Different projects to implement and test IoT in buildings.”* *“Upscaling of digital twins in buildings and infrastructure.”* *“EU research and development project.”* *“Creation of digital twins/cyber physical systems for interoperability and prediction techniques about performance.”*

“Implementing tools for facility management."

“Integrating new algorithms to optimise building in all phases; construction, management.”

“To test in a research project.”

“Power consumption, security, structure durability and failures.”

“Research projetcs and our own buildings.”

“Real scale.”

4.4 Analysis

This section will describe the analysis of the survey that was distributed to experts in industry (Alshammari, Beach and Rezgui, 2021a). The goal of the activities focused on identifying the obstacles to the adoption of access management for digital twins/CPS in the built environment and improving the built environment.

Overall, the survey revealed that;

- 78.6% of organisations use log-in details for authentication as a means of access required to manage data for digital twins/CPSs.
- 77.8% of organisations control the availability of data.
- 61.5% of organisations do not possess the tools and processes to identify and prevent sensitive data from leaving the digital twins/CPSs.
- 60.6% of organisations do not deploy digital twins in any project,
- 50% of the respondents suggested that this was due to the cost.
- 39.4% of organisations deploy digital twins in the building operations area as well as data analysis and urban design development.
- 57.1% of organisations do not have a dedicated cybersecurity team to manage and design digital twins/CPSs because of a lack of expertise.
- 57.1% of organisations lack the ability to monitor digital twins/CPSs to detect anomalous activities.
- 54.5% of organisations plan to use digital twins in different areas in future.
- 51.5% of organisations do not use the CPS/IOT.
- 63.2% of organisations lack data protection and data security.

- 46.9% noted that increasing the availability of training in this area is extremely important to encourage adoption of both digital twins and CPSs in the built environment and cybersecurity frameworks in the built environment.
- 35.5% stated that BIM specifications becoming IoT-compliant is important to enable the adoption of digital twins/CPSs in the built environment.

The survey has also provided insight about a problem faced by the industry, which is that there is not a single, established standard because each platform specifies its own protocols, encodings, and APIs. Understandably, this gives rise to interoperability issues, thereby complicating efforts to manage access control across various providers and their platforms. This same problem affects cybersecurity provision regarding platforms and distributed services in the built environment.

A second issue is that keeping digital twins for entire urban districts up to date is said to be very difficult. Furthermore, the data needed for digital twins is not often in the hands of a single owner but spread across many stakeholders. This makes the data vulnerable to loss.

In terms of obstacles and blockers, the survey has told us that, ideally, BIM specifications would form the basis for smart building technologies, but BIM specifications were never intended to support smart buildings. Rather, BIM was only ever intended to facilitate data being shared among applications. As such, if BIM is to become compliant with the IoT, it must be amended by incorporating effective cybersecurity. This requires new technological elements governing how information is utilised in information exchanges. Cybersecurity must become embedded in digital twins, physical objects incorporating the IoT and information models such as BIM.

In the future, if BIM is to be put to work in smart buildings, this will require the use of the IoT. Several IoT platforms e.g., FIWARE (Fazio and Celesti, 2015) have been devised by researchers but none of these offers the ability to integrate seamlessly with BIM models. This is due to the fact that while these platforms utilise BIM models for spatial elements, IoT related information within BIM models are not considered. Efforts to address the cybersecurity concerns associated with BIM have seemingly overlooked the need to be able to operate secure servers.

Digital twins offer exciting opportunities regarding the optimisation, simulation, forecasting and monitoring of CPSs. Researchers have sought to enhance the reliability of CPSs but there is now growing recognition of the need to defend against cyberattacks. Be that as it may, the process of incorporating cybersecurity into digital twins intended for use in the built

environment is highly problematic. There is a need for digital twins to ensure the secure and identity of their true twin (Alshammari, Beach and Rezgui, 2021a). Therefore, industry looks forward to developing smart buildings through IoT compliance with sensors.

However, the results from this survey has shown it still lacks a cybersecurity model for digital twins that works suitably and safely. Those responsible for overseeing investment in smart buildings and the application of BIM when designing and managing assets must have a grasp of the latest cybersecurity threats and mitigate any risk to the common data environment. Otherwise, the asset's cybersecurity could be jeopardised because intellectual property could be lost, or the systems associated with the asset could be breached (Alshammari, Beach and Rezgui, 2021a). Based on these obstacles, numerous recommendations can be made for the provision of a cybersecurity framework in the built environment.

From the survey and the literature review, a series of recommendations were derived to enhance access management frameworks for digital twins, and these are as follows:

- Develop a framework to provide access controls and SSO across built environment services that leverage digital twin and BIM data.
- Enhance BIM standards along with evolving digital twin and future city standards to fully integrate support for IoT and access management considerations such as encryption and access control.
- Provide training to enhance skills to improve adoption of cybersecurity for digital twins/CPSs in the built environment.
- Enhance relevant technology such as the IoT and CPS to improve adoption of access management for digital twins/CPSs in the built environment.
- Develop and specify a reference architecture for security aware applications in the smart built environment to promote adoption of access management for digital twins/CPSs in the built environment.
- Smart grid security to enhance adoption of access management for digital twins/CPSs in the built environment.
- Expand BIM specifications to become IoT-compliant for the adoption of access management for digital twins/CPSs in the built environment.

4.5 Summary

This chapter has described the industry survey conducted to: (a) understand the adoption of the cyber-physical system regarding the built environment; (b) understand the adoption of digital twins in the built environment; (c) determine the obstacles to the adoption of access

management for digital twins/CPS in the built environment encountered by experts in this domain. The survey was distributed via the ECTP, social media and individual contacts with individual experts.

The survey was conducted to reveal the research obstacles and enhance the built environment.

This chapter has also answered the second research question: *What are the current obstacles to tackling access management threats to the built environment in CPSs?*

In answering this question, this chapter has identified the following obstacles: a lack of data security; cost; the ease of adopting access management; the tools and processes needed to identify and prevent the loss of sensitive data; the ability to monitor DTs/CPSs to detect anomalous activities; the lack of a single, established standard because each platform specifies its own protocols, encodings and APIs; and the fact that the data needed for digital twins often is not in the hands of a single owner but spread across numerous stakeholders.

Chapter5: Access Management Framework for Digital Twins

Chapters 2 and 4 have identified the importance of access management for digital twins in the built environment to support multiple services in smart cities. Furthermore, the built environment encompasses various domains that include many organisations and assets. Specifying an access management framework to secure data from digital twins is thus critical to the potential development of secure built environment tools across a variety of use cases. In this chapter, the overall access management framework proposed by this this along with a semantic approach to deliver it is discussed in depth.

This chapter forms part of phase 4 of this research methodology. It specifies an access management framework to overcome the cyber-security research gaps for built environment use cases. Specifically, these gaps include:

- BIM standards are not currently compliant with IoT standards in the areas of access management, there are no specific standards governing how IoT related information can be represented within an IFC model. Therefore, BIM standards must be amended to incorporate effective access management concepts. This requires new technological elements governing how information is utilised in information exchanges. Access management must become embedded in digital twins by incorporating IoT-related concepts in information models such as BIM.
- Several IoT platforms e.g., FIWARE (Fazio and Celesti, 2015) integrate with BIM yet none of these offers the ability to integrate seamlessly with BIM models. This is due to the fact that while these platforms utilise BIM models for spatial elements, IoT related information within BIM models are not considered. Efforts to address the access management concerns associated with BIM have seemingly overlooked the need to be able to operate secure servers.
- Incorporating access management into services operating on digital twins in the built environment is highly complex. To enable digital services driven by digital twins, 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 (authorisation and authentication). The complexity originates from the different categories of users wishing to use data and actuate services from digital twins. These digital twins have differing security requirements based not only on the type of the assets, but the scenario of its use and the impact the action on the digital asset will have on the physical asset.

This chapter focuses on developing the semantically specified access management framework that will be used to answer the following research question:

RQ3: *What are the key requirements for a semantically specified access management framework suitable for the built environment?*

This RQ will be answered by:

- Creating a semantically defined access management framework for the built environment. The reason for creating a semantically defined access management framework is that it provides formalised semantics to management access management concepts. This in turn then allows interoperability between various existing standards / tools used within the built environment enabling them to leverage the defined access management concepts.

- Formally specifying the key elements of the framework through an ontological modelling method which formally represents 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 robust. Furthermore, at operation time it enables easier management of access management configuration and settings dynamically across an assets life cycle. (Burov, Mykich and Karpov, 2021).

5.1 A Semantically specified access management framework

A smart city underpinned by a cyber physical system in conjunction with the provision of information from the IoT, BIM and data mined from the Internet sources and direct from citizens can provide an intelligent solution to improve the quality and performance of urban services such as transportation, energy, and weather. These intelligent solutions will effectively aid the operation of an urban area, as seen in Chapters 2 and 4.

Although such innovations are thought to significantly enhance infrastructure in the built environment, they often pose technological challenges that must be addressed. Indeed, the diversity of data sources and knowledge modelling could restrict decision support capacity (Darif, Chaibi and Saadane, 2019; Kuster, Hippolyte and Rezgui, 2020). There is also the significant issue regarding the need to defend against cyberattacks and properly enforce access control (Howell and Rezgui, 2018). Integrating access management into digital twins for use in the built environment has so far proved extremely problematic. The safety of Digital twins is needed to ensure the safety and identity of their physical twin. Methods and data

models for ensuring efficient protection across platforms, domains and scales are needed (Hashem *et al.*, 2016; Rosique, Losilla and Pastor, 2017). More specifically, there is the need to integrate IoT Devices and cyber-physical systems, existing built environment services, existing security standards, digital twin, and BIM datasets as well as newly developed user interfaces and the actors who use them. Each of these areas already has existing implementations with their own semantics, data structures and APIs (see Figure 5.1).

Thus, to integrate these disparate efforts into a cohesive access management approach, the current study adopts a semantic modelling approach to formalise semantically the concepts involved and relate and align them to the existing concepts and existing ontologies within these domains.

Figure 5.1 shows the semantic inter-relationships within the proposed access management framework. This figure illustrates how the semantically defined cybersecurity framework will identifies the key areas of semantics needed to provide access management for digital twins and then integrate these previous isolated semantic elements into a cohesive semantic model.

Thus, this framework will utilise semantic web technologies to integrate existing cyber security standards from other domains to existing work in the area of modelling physical city artefacts such as structures, people, and processes, along with the digital services that operate on them.

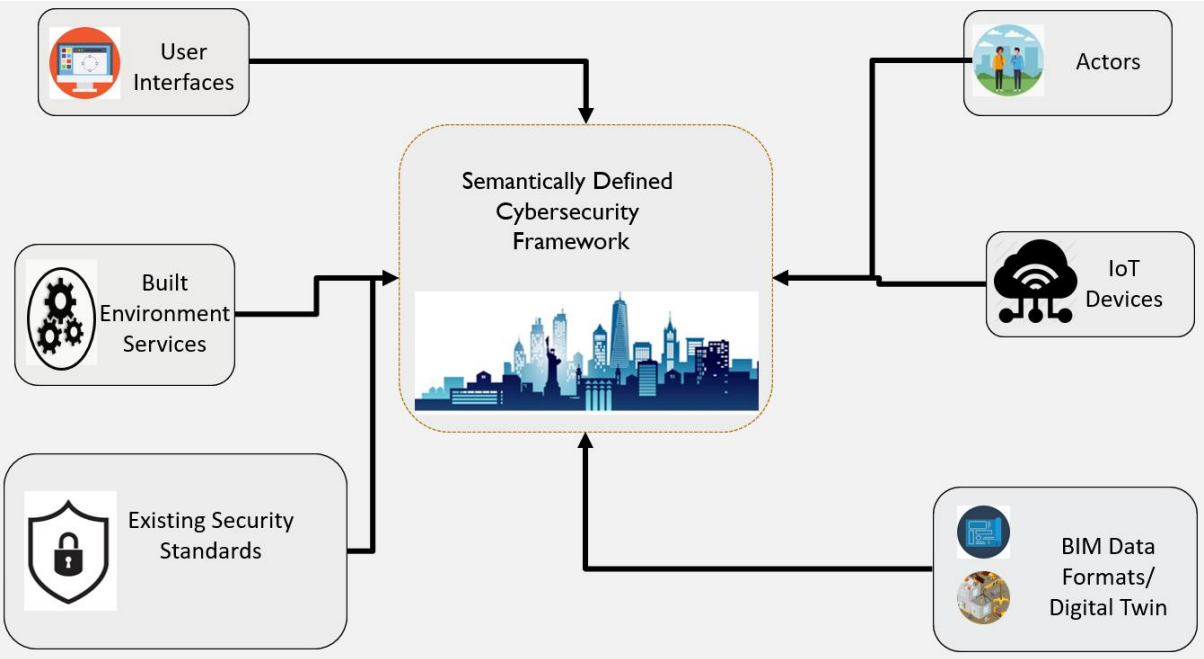


Figure 5.1 Semantically defined access management framework

This work adopts the concepts of semantic modelling and ontologies as they are useful tools for modelling the formal relationships that must be formed between access management and built environment concepts. More specifically, ontologies define an explicit domain-specific semantic schema that can explain real-world concepts and relationships. Heterogeneous sources may be aligned over similar concepts, enhancing interoperability because information is treated in terms of its formalised semantics. Furthermore, because the user of the ontology does not need to understand the data structure itself (only the semantics), this approach greatly aids knowledge exploration and integration (Dibley *et al.*, 2012). Finally, semantic web technologies allow for the creation of linked data. They have the potential to link the requirements of the assessment framework to local policies (Kuster, Hippolyte and Rezgui, 2018). Currently, semantics have been used to great effect in the area of smart manufacturing, smart buildings and smart grids during the engineering and operation of CPSs (Ekaputra, 2020). The following sections describe the developed access management ontology along with the methodology used to develop it.

5.2 Ontology development methodology

Due to the fact that an ontology is, by definition, an integrative information system that can also integrates other ontologies, a precise approach must be followed in order to construct a linked knowledge network efficiently. This section details the chosen technique: the NeOn technique. The NeOn methodology has been selected for the following reasons: (a) ease of knowledge; (b) scenario-based methodology; and (c) accessibility of supporting documentation (Suárez-Figueroa, Gómez-Pérez and Fernández-López, 2015). As a result, the NeOn technique was chosen to create the access management for digital twins in the built environment ontology (Suárez-Figueroa, Gómez-Pérez and Fernández-López, 2015).

The NeOn methodology for ontology development (see Chapter 3) uses semantic web technologies to "unify" heterogeneous sources of information by integrating and aligning reusable existing knowledge within the ontology design phase. This methodology demonstrates how semantics can truly ‘unify’ heterogeneous sources of information (Hou, 2015)

The main goal of NeOn is to deliver a comprehensive ontological development framework (Hippolyte *et al.*, 2018). This consists of (Suárez-Figueroa, Gómez-Pérez and Fernández-López, 2015):

- A glossary describing the NeOn processes regarding ontological development and related activities.

- Nine scenarios for ontological development.

-There are two life-cycle models that outline the processes and activities of ontology development.

- A set of guidelines for conducting research (Baonza, Pérez and Villazón, 2010).

Figure 5.2 depicts the NeOn methodology life-cycle with solid black components indicating obligatory stages and dotted components indicating optional steps, depending on the scenario and the dotted components refer to optional steps and the dotted arrows refer to an optional iterative loop. This figure depicts the nature of the process of ontology development in which the designed model must be enhanced and re-engineered iteratively.

After determining the obstacles, they are then analysed and evaluated according to the NeON methodology. Based on such analysis, this chapter defines the built environment cyber-security framework required to solve the previously elicited obstacle. The work in this chapter follows the phases from Figure 5.2 to create the access management framework for digital twins in the built environment:

Phase 1 (Initiation): This phase produces the formal ontological requirements specification. It is driven by the previous literature review (Chapter 2), survey results (Chapter 4) and analysis of a set of built environment case studies (described in Section 5.4).

Phase 2 (Re-use phase): This stage analyses existing ontological resources and determines how they can be re-used within the developed ontology. This will factor in existing semantic resources that already exist in the built environment and access management domains (described in Section 5.5).

Secondly, non-ontological resources will be examined and then semantised and re-engineered to align with the existing ontological resources. This process is conducted for the four case studies used to derive the requirements (described in Section 5.6). They are primarily studied to determine the terminologies and key concepts that will be useful in the ontology.

Phase 3 (Design): This consists of the final design and development of the ontology driven by the requirement specification and the re-engineered ontological and non-ontological resources (described in Section 5.7).

Phase 4: Implementation; The developed ontology will be implemented and validated on a digital twin case study within university buildings (described in Chapter 6).

The implementation of this methodology is described in the following sections.

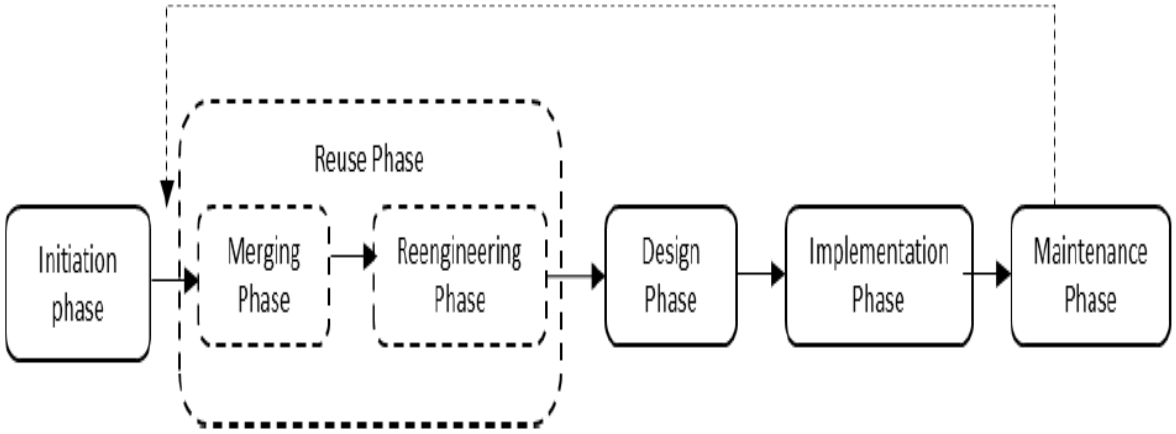


Figure 5.2 *NeON methodology* (Suárez-Figueroa, Gómez-Pérez and Fernández-López, 2015)

5.3 Built environment case studies

This section presents the case studies that were used to drive the requirements engineering process and are subsequently formalised into ontological resources.

This process was initiated by studying the general terminology used in the built environment which is defined as "*the human-made environment that provides the setting for human activity, including homes, buildings, zoning, streets, sidewalks, open spaces, transportation options, and more. The human-made space in which people live, work and recreate on a day-to-day basis*" (Gray, Zimmerman and Rimmer, 2012).

The terminology derived is summarised in Table 5.1. This table has been derived from a study of the relevant literature (Chapter 2) to form a list of basic concepts that act as a starting point for a set of terminology to feed into the ontology developed.

Table 5.1 Built environment components

City	**District**	**Street**	**Building**

• Local Government Information • Population • Address • List of Districts • List of Buildings • List Streets • List of Organisations • Name	• Address • List of Buildings • List of Streets • Name	• Has Pavement • Traffic Light • Traffic Level • Pollution Level • Noise Level • List of Buildings • List of Streetlight • Has Bike Lane • Number of car lane • Number of Parking Space • Parking Metered • Name • Has Bus Stop • Road Sign • Has Waste Containers	• Owner • Address • Postcode • Building Number • Number of Floors • Number of Rooms • Number of occupants • Purpose • Building Signs • Max Occupants

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 (Chimay, 2020). In the absence of detailed examples of real digital twin use cases, this thesis utilised use cases of various more common smart systems that re commonly employed as part of a wider digital twin systems: smart parking system, attendance management system, access door system and smart Air-conditioning system.

Each of the case studies is described in the following subsections using a series of tables (see Appendix B), each of which shows:

Data description: the definition of the concepts, what data is covered and its type.

Data controller: who the system administrator is; the individual who holds authority over the data.

Confidentiality: Refers to who has access to view the data.

Integrity: Refers to who has access to edit the data.

Availability: Refers to restrictions/requirements placed on how the data must be made available.

Notes: Any additional information about the data.

5.3.1 Smart parking system

The smart parking system refers to end-users (students, staff members) who are provided with a custom mobile application (parking application) (Canli and Toklu, 2021). This application enables them to find the available parking spaces at a university, gives appropriate directions to the target parking spot, makes a reservation, checks the remaining parking time, and receives a notification when the parking time has expired. First, the user is required to connect to the app through their mobile telephone (Beetham *et al.*, 2014).

5.3.2 Attendance management system

Attendance management keeps track of students' attendance via their fingerprints. This system records students' attendance by putting scanning their fingers on the device. As for non-students, the system will reject the fingerprint (Shoewu *et al.*, 2012; Siksha ‘O’ Anusandhan , Bhubaneswar, 2020).

5.3.3 Access door system

The access door system allows users of a building to access the security doors in the building. Users should pass their card over the device. Those who do not hold a card cannot access the building via the door (Moukhliss, Filali Hilali and Belhadaoui, 2019).

5.3.4 Smart Air-conditioning system

The smart air-conditioning system (Moukhliss, Filali Hilali and Belhadaoui, 2019) allows the user to control the air conditioning in the building. The staff member in the building should insert their ID into the device to control the air-conditioning settings.

5.4 Requirement Specification

This section defines the specification of the requirements for the access management ontology. As previously described, the NeOn methodology is utilised to develop the built environment access management ontology (Howell, Beach and Rezgui, 2021). Within the NeOn methodology, the Ontology Requirement Specification (ORS) (Tapia-Leon *et al.*, 2019)

is the first step. It is a critical step that helps to define the domain semantic modelling limits and places a strong emphasis on appropriate information resources. It necessitates determining: (1) the goal of the ontology being developed; (2) the ontology's possible uses and users; and (3) the criteria that the ontology must satisfy (Vajpayee and Ramachandran, 2019).

Firstly, the ontology's main goal is to reflect the integrations required by the access management framework in formalized semantics. This is providing integration between physical built environment assets, IoT devices, cyber-physical systems, current built environment services, existing security standards, digital twin and BIM datasets, as well as newly developed user interfaces and the actors who use them.

Thus, the access management framework for digital twins in the built environment will include formalised semantics for implementing access control, data confidentiality and integrity, and Single Sign-On (SSO) across built-environment services for use in digital twins and supporting BIM data. The formal specification of access management ontology for digital twins in the built environment supports this. This formal specification is documented in Table 5.2.

The final step is to identify the criteria that the final ontology must satisfy. Following the NeON methodology, this will be achieved by defining the competency questions and is described in the following subsection:

Table 5.2 NeON Ontology requirements specification

Ontology requirements specification
Purpose: An access management ontology for digital twins/cyber-physical systems in the built environment.
Scope: The semantics need to integrate the disparate semantics of the existing cyber security standard from other domains with the actual physical city artefacts such as structures, people and processes, along with the digital services that operate on them.
Level of formality: Rigorous formal ontology specified in OWL.
Intended users: The primary users of the ontology are software developers, sensor developers, device developers and anyone who wants to develop a piece of (software, service, smart device CPS or digital twin) in the built environment.

Intended uses: Ontology is developed using semantics derived from a series of case studies such as smart parking (see Section 5.3.1), the attendance management system (see Section 5.3.2), the access door system (see Section 5.3.3) and the smart conditioning system (see Section 5.3.4). However, the intended use is any use of services in the built environment with an access management requirement.
Group of competency questions: Competency questions were derived based on the pro-glossary of terms and the case studies listed in Tables (see Appendix C).
Pro-glossary of terms: The terms are inserted in Tables (see Appendix C).

5.4.1 Competency questions

Competency questions are a helpful way to establish the complexity of an ontology because they list a collection of questions that an ontology-based knowledge should be able to address (Hippolyte *et al.*, 2018; Vajpayee and Ramachandran, 2019; Tapia-Leon *et al.*, 2019; Tarasov, Seigerroth and Sandkuhl, 2019).

The competency questions have been categorised into five groups (IoT devices, built environment data format, actors, built environment services, and security standards), which correspond to the areas of access management that this semantic model is seeking to integrate. the collection of competency questions concerning the various elements and components of the built environment such as people, actions and objects, and their effect on security efficiency (see Appendix C).

Thus, these competency questions focus on essential concepts which must be included in the ontology.

5.5 Analysis of existing ontological resources

Access management is a relatively new field that aims to secure digital infrastructures against vulnerabilities or threats (Górka, 2021). Although knowledge of access management 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 (Górka, 2021).

Furthermore, the range of contributions provided by diverse professionals in this sector has steadily established a wide knowledgebase of access management across different disciplines. Some of these efforts have led to the development of ontologies to help define, represent and organise a vocabulary of concepts in their given field (Ciberseguridad, 2021).

When constructing a new domain ontology, the NeOn approach encourages the reuse of existing ontological and non-ontological tools. The resulting semantic model is based on defined ontologies and is therefore consistent with other context ontological tools. The study of tools that can be reused has been refined by listing potential uses and users and posing competency questions. It is possible to categorise the various concepts discussed for a future ontology.

Thus, is an important element of the NeOn methodology being followed by this work, to re-use, where possible, existing ontological resources. The main benefit of ontology reuse is that it is already formalised, thereby saving time and money during the creation stage of ontology development. Furthermore, reusing current ontologies follows the ontology principle of the creation of an integrated knowledge base. When an ontology developer has complete freedom, most experts advise reusing an ontology whenever possible.

Simperl (2009) outlined the key steps involved in reusing ontologies efficiently:

(1) *"Discovering ontologies"* (Simperl, 2009): there are already a large number of ontologies available for different domains. The use of ontology search engines such as Swoogle, Watson, or the Protégé OWL library (Beniaminov, 2018) helps to search for qualified ontologies.

(2) *"Selecting those to be reused"* (Simperl, 2009): after deciding on a collection of ontologies, the developer must determine those that are compatible with the newly created one. Ontologies may be reused completely or partially based on the aspect they cover, with ontology requirement specification guiding the selection. In order to efficiently select useful ontologies, the ontology requirements specification and competency questions must be well-defined. It is worth noting that broad ontologies appear to overgeneralise, leaving out particular domain aspects, whereas extremely comprehensive ontologies express extensive and difficult-to-understand information. As a result, the author must have a clear understanding of the degree of abstraction they want to offer their model, as well as weighing up the pros and cons of reusing existing ontologies versus creating one from scratch.

(3) *"Customisation of relevant ontologies"* (Simperl, 2009): after the collection of ontologies, the developer often has to change them to fit the desired purpose. For example, one may add or delete axioms, restructure the architecture or move from one language to another. The ontologies may be re-engineered or reused as is, depending on the ontology requirements specification.

(4) *"Integration into an application ontology*" (Simperl, 2009): the final step is to align the various domain ontologies into a single new one. The author must use equivalences, possible limits and/or properties to connect various concepts. The final model must then be checked for accuracy and reworked iteratively between steps 3 and 4 until it is sound.

The remainder of this section describes the existing ontological resources that are considered as part of the development of the built environment access management ontology. The ontology reflects the semantic integration required to achieve access management. This includes resources and policies but also permission between physical built environment assets, IoT devices that 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.

5.5.1 Built environment resources

Ontologies for the semantic representation of smart buildings were discussed in Section 2.3. As a result, this feature of the ontology can be applied to the access management framework. To build the ontology in the field semantic landscape, future possible connections with other built environment ontologies may be researched later. The access management concept will be integrated in the built environment application ontology.

One of the existing built environment resource that was considered is the Cardiff Urban Sustainability Platform (CUSP) ontology (Hippolyte et al., 2018). This ontology forms that semantics that underpin the CUSP platform which is being developed by Cardiff University as a decision-making tool that offers in-depth urban analytics through an engaging interface. (Hippolyte et al., 2018). As this platform is semantically driven, this offers us a great source of existing ontological resources. More specifically these semantics include:

- Built Environment Spatial Modelling (including a building, city and district modelling semantics)
- Integration of this spatial model with sensing ontologies (See Section 5.5.2)
- Semantic modelling of district energy resources, i..e district heating, smart grids and renewable energy sources.
- Semantic modelling of services that operate upon the platform i.e., AI algorithms, optimisation algoritms and reasoning services.

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.

An additional important existing ontological resource is ifcOwl. This is the most common ontological resource in the built environment and is derived from the IFC format. This format has been designated as the preferred standard for building data interchange (Pauwels, Zhang and Lee, 2017).

As a result, one of the primary integrations that can be enabled by this ontology is linking access management concepts with ifcOwl to enable the required integration between physical built environment asset data, IoT devices and existing security standards.

5.5.2 Sensing resources

The semantic description of a sensor, its findings and the entire sensing process is an important part of the ontology. The user should be able to capture the information provenance and flow, whether by focusing on performance or measurement. Ontologies like the Observation and Measurements ontology (O&M) (Jiang, Kuhn and Yue, 2017; Cox, 2017), the SSN/SOSA ontology (Pal *et al.*, 2020), or the SAREF ontology (Thakker *et al.*, 2020) are recognised frameworks for the semantic modelling of observations 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" (Haller *et al.*, 2018). SAREF is a model that defines concrete devices and smart appliances in the built environment (Petrova-Antonova and Ilieva, 2021) as well as the properties that they monitor. Despite the fact that 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 SSN ontology tends to be the most promising candidate for the development of the USA ontology because it incorporates the classification of sensors and their observations at a higher level of abstraction, allowing for more versatile modelling. 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.

Figure 5.3 depicts a selection of the most important classes generated in SSN for the USA ontology (Jiang, Kuhn and Yue, 2017).

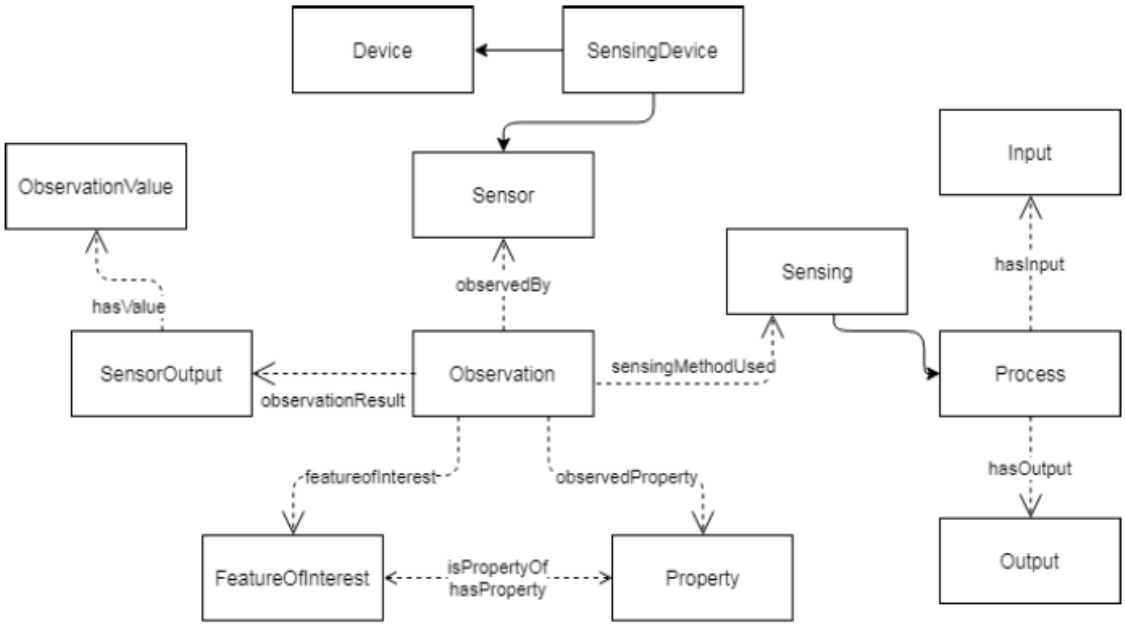


Figure 5.3 *The SSN ontology, key concepts and relations* (Jiang, Kuhn and Yue, 2017)

The triple observation, property, and feature of interest is at the heart of the schema, just as it is in O&M, providing a detailed definition of a specific capture of an entity function. The observation produces a SensorOutput which is correlated with an ObservationValue. A sensor, which can be of type of device, performs the observation. This results from a SensingMethod that is defined in terms of the inputs and outputs. Sensors can also be grouped into a framework that is hosted by a shared platform and deployed according to a set of rules.

After two years of development based on the 2011 version (Taylor *et al.*, 2019), the SSN ontology was revised in October 2017 (Taylor *et al.*, 2019). As a result, the USA ontology is based on the 2011 edition but configurations between the two versions were considered when creating the updated version.

Finally, the calculated values are often linked to a measurement unit. The Quantities, Units, Dimensions, and Data Types (QUDT) ontology (Seeger, Deshmukh and Broring, 2018) has already been used by NASA to model them semantically.

5.5.3 Urban objects resources

One of the criteria is the portrayal of people and objects in the urban setting. As a result, sensors can be pinpointed to specific objects and the function of value that they detect can be described and categorised as one of those objects. “Urban objects” encompass a wide range

of items, from buildings and their interiors to the roles and furniture of urban environments, as well as the people who communicate with this community.

The buildings and their elements have already been semantically modelled using the ifcOWL ontology (Pauwels, Zhang and Lee, 2017). The Industry Foundation Classes (IFC) standard is a data structure and an exchanged file format for BIM data (Pauwels, Zhang and Lee, 2017), and IfcOWL is the RDF representation of it. The ifcOWL ontology is a wide ontology with 1,230 classes, 1,578 object properties, and 5 data properties that allow 21,306 axioms and 13,649 logical axioms to be created. This involves, for the most part, the geometries of the existing buildings and lists of Cartesian points, polylines and other similar items (Pauwels *et al.*, 2017). In order to introduce a more flexible version of the ifcOWL, a modular version was developed to simplify or even delete the geometry (Pauwels *et al.*, 2017; Pauwels and Roxin, 2016). IfcDoor, IfcBeam, IfcWindow, IfcRoof, IfcWall, IfcOccupant, IfcMaterials, IfcBuildingStorey, IfcBuilding, IfcSpace, and IfcFurniture are only a few examples of the construct components. Overall, the ifcOWL ontology can semantically define all of the components of the building world, from component geometry to processes and people, and how they interact. It may be beneficial to locate a ssn: in this case. For example, in a specific ifcOWL:IfcSpace or ifcOWL:ifc, the ssn is the structure: A ssn:FeatureOfInterest of a ssn:Observation.

Finally, the Friend-Of-A-Friend (FOAF) ontology is a semantic model for explaining individuals, their actions, and their relationships to other people and objects in the digital world (Brickley and Miller, 2014). It can be used to semantically classify the active agents in charge of specific aspects. Indeed, certain security requirements can be related to specific procedures that must be carried out to strengthen them. In turn, those interventions can be linked to an agent or service provider. As a result, the FOAF ontology enables the service provider to provide digital information. Classes such as foaf:Organisation, foaf:Agent, and foaf:Person, as well as their real-world objects like foaf:name, foaf:age, foaf:knows, and foaf:member, and their digital environment objects like foaf:mbox, foaf:workplace, form the core of the ontology.

5.5.4 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 (Charpenay and McCool, 2021).

In the context of access management, the primary security standard being examined is the OAuth 2.0 authorisation “framework.” Existing semantic resources in this area include that of

Charpenay and McCool (2021) and this ontology formalises elements of semantics related to a web of things. However, it provides no specific built environment concepts.

5.6 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 (Chun *et al.*, 2020).

To attempt to make maximum re-use of existing non-ontological resources available the four case studies previously descried will be considered as non-ontological resources and will be used for the extraction of domain information from them. They are primarily studied to determine the scope of the domain, as well as to learn the terminologies and key concepts that will be useful in the ontology.

To perform this extraction of terminologies and key concepts, this section will present the formalisation of the case studies as tables and class diagrams and the key concepts will be extracted from them.

5.6.1 Class diagrams

This section presents a series of class diagrams that show how the semantics of the various use cases (smart parking system, attendance management system, access door system and smart conditioning system) have been formalised. The diagrams categorise these in accordance with the segments of the access management framework defined in Figure 5.4 as follows:

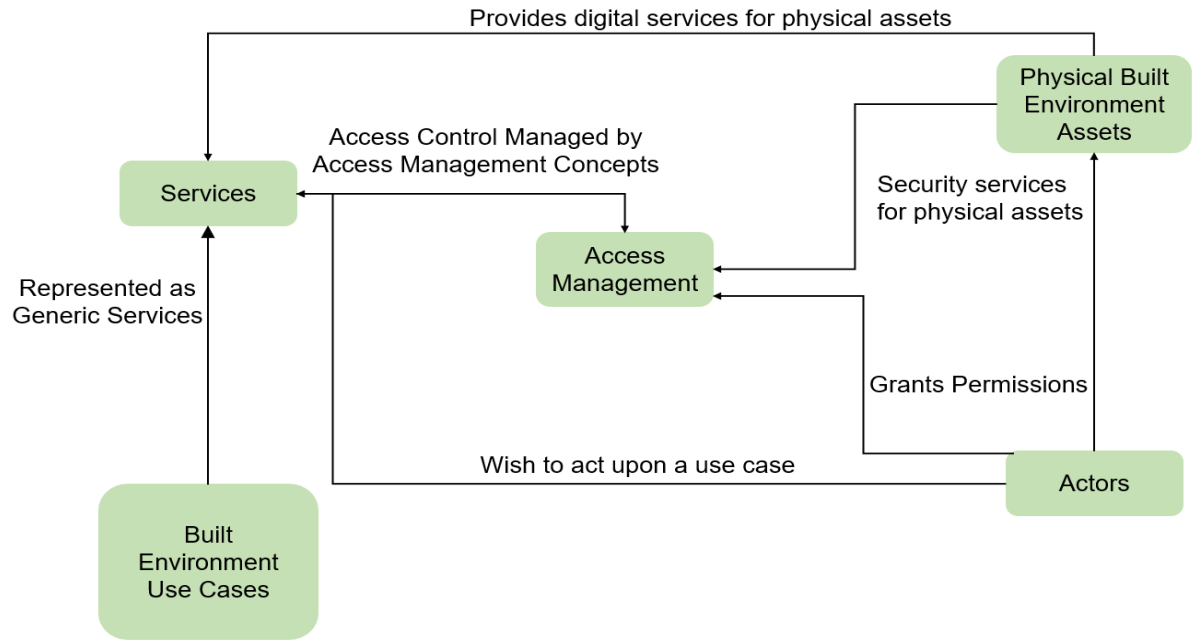


Figure 5.4 Access management framework

CUSP represents the IoT Devices in the system, access management represents the key required concepts from existing security standards (i.e., OUATH2), and service represents the digital services employed. Additionally, the diagram has a segment representing specific concepts relating to that use case (see Appendix D).

5.7 Access management ontology

Based on the requirements specification, existing ontological resources, and existing non ontological resources, the access management ontology has been developed. This section presents various visualisations of this ontology. These are shown in Appendix E. Due to the large number of classes and properties created, only those from the Smart Parking case studies are shown

Appendix E includes four figures. Figure 1 shows the classes within the smart parking case study, Figure 2 and Figure 3 show the object and data properties for these classes. Finally, Figure 4 shows the individuals of the smart parking case study.

More specifically the classes/properties and individuals specified in these figures include the generic access management concepts. These include: Policy, Actor, Role, Permission, and Resource. These concepts allow the definition of a set of flexible permissions. A user is assigned to a role. At the same time resources (services or physical devices) provide.

permissions that conceptualise what functionality that they can perform. Then a policy provides a mapping between user/role and permissions for a given resource.

5.8 Summary

Interoperability is a critical component of achieving holistic and accessible services in a smart city. As a result, strategies to deal with this problem must be considered. Fragmented semantics across differing contexts are notorious for causing interoperability issues and creating obstacles for software developers and integrators. One method that has had great previous success is the use of ontologies that integrate the disparate semantics between multiple domains.

In the context of establishing an access management framework for the built environment this section has described the access management ontology that has been developed to enable the interoperability between physical built environment assets, IoT devices, cyber-physical systems, current built environment services, existing security standards, digital twin and BIM datasets, as well as newly developed user interfaces and the actors who use them.

This chapter has addressed the creation of the semantically specified access management framework, the associated ontology development methodology, built environment case studies, requirement specification, competency questions, analysis of existing ontological resources, built environment resources, re-engineering of built environment non-ontological resources, class diagrams and access management ontology.

Overall, the evidence presented in this chapter has helped to answer the following research question:

RQ3: *What are the key requirements for a semantically specified access management framework suitable for the built environment?*

This has been achieved by specifying and subsequently developing an ontology. This ontology forms the key integration between of the existing semantic resources of the domains involved. This ontology will be fully validated in the next chapter with the verification and validation of the ontology.

Chapter 6: Access Management for Digital Twins in Built Environments Framework Verification and Validation

6.1 Introduction

Chapter 5 identified the specification of an access management framework to overcome the access management research gaps for building environment use cases. Chapter 5 focused on the development of the semantically specified access management framework, primarily through an iterative ontology design to integrate disparate semantics across the multiple domains involved.

This chapter forms part of phase 5 of this research methodology. It formally validates the access management framework and associated ontological modelling, and fully addresses the following research question:

RQ4: *Can the current security processes employed by CPS and digital twins be improved to address the access management requirements of digital twins in the context of the built environment?*

This includes:

- Validating semantic representation against the compliance questions previously elicited.
- Testing its functionality on a new case study. The semantic access management framework is initialised for this case study and tested and validated.

This process includes testing the ontologies compatibility with the required concepts for the built environment such as the provision of correct SSO and access control.

6.2 Verification & Validation methodology

The validation methodology employed in this chapter consists of the following stages:

1. Technical verification against competency questions
2. Validation utilising a use case deployed on the Cardiff University CUSP platform

Technical verification **against competency questions:** This step of the process entails verification against the created ontology that all competency questions are answerable via the ontology. This is conducted through a manual comparison of the ontology against the given competency questions (Vajpayee and Ramachandran, 2019).

Validation utilising a use case deployed on the Cardiff University CUSP platform: To conduct this element of the validation, the access management ontology is integrated into the existing CUSP platform (further details provided below) and will thus be used and validated on one of the demonstrators already running on the platform. This will validate the ontology by performing the following tests (based on the data already present within the CUSP platform):

- Validating that the ontology can adequately represent the security requirements of the selected CUSP use case.
- Validating the ontology functions correctly in assigning and provisioning access rights to build environment services, thus enabling SSO.

The CUSP platform is a decision-making tool driven by semantic models. It consists of a series of analytic components including AI and optimisation modules, all driven by a set of semantic data-stores. The platform interface uses a web-based view that provides access to data and access to existing urban datasets (see Figure 6.1). As a research prototype, the CUSP platform does not currently possess an in-built security framework.

CUSP has been utilised for a variety of cases including:

1. Managing services at Cardiff University
2. Energy monitoring for university and local authority buildings
3. Water network management (Zhao, Beach and Rezgui, 2018)
4. Energy planning and flexible energy management at an industrial park (Hippolyte et al., 2018)

As part of this validation use case (1) will be modified and the ontologies developed in Chapter 5 will be instantiated and integrated within the CUSP platform. This use case has been selected because it is the use case that has the most data available and it is free of restrictions regarding how its dataset can be used.

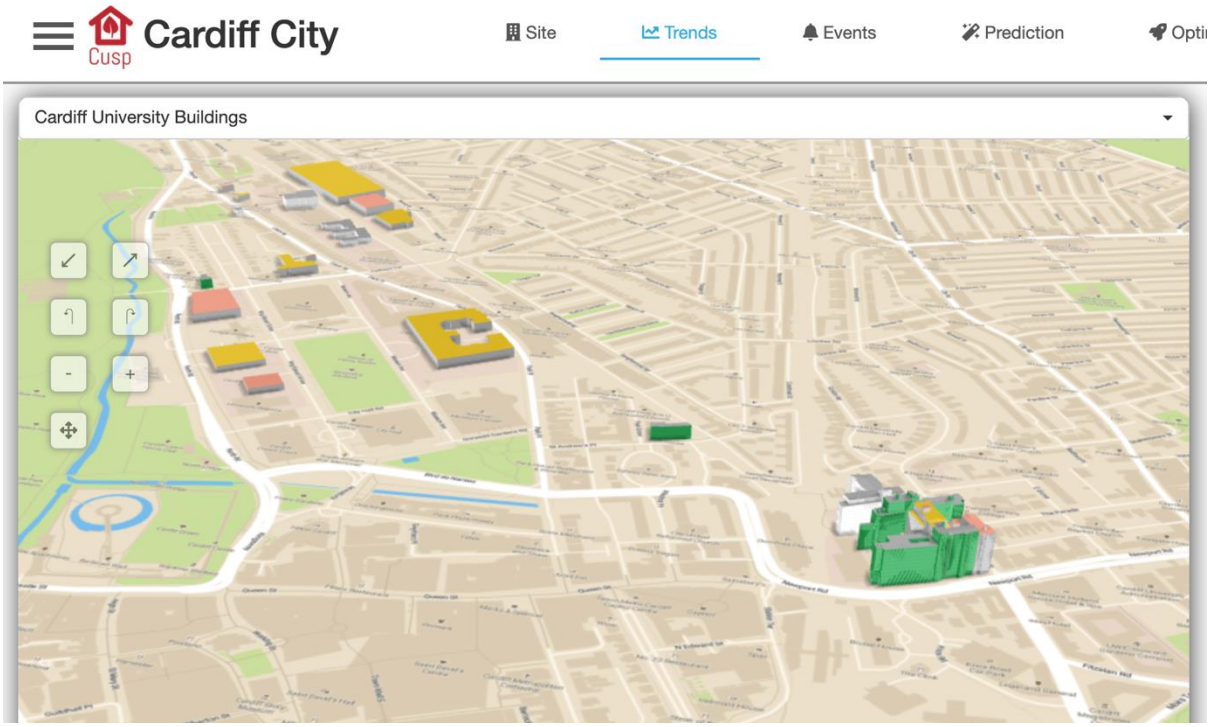


Figure 6.1 Cardiff Urban Sustainability Platform (CUSP)

6.3 Technical verification against competency questions

The competency questions have attracted terminologies that can help when searching ontological resources by focusing on crucial concepts that must be involved. It is to assure that the ontology developed meets the requirements from the requirement specification. The current study identifies five crucial components that must be present: IoT devices, the built environment data format, actors, built environment services, and security standards; the representation; the representation of the object as it interacts with the city dynamic, from the built environment to services.

Table 6.1 Smart parking access control competency question verification

Competency Question	**Response**
What building, and physical location within a building, is a given sensing device associated with?	This has been met through the implementation of the Space class and the hasLocation object property that relates it to the Sensor class. This is provided by existing CUSP ontologies.
How many sensor devices does a given space have?	This has been met through the implementation of the Space class and hasSensor object

	property. This is provided by existing CUSP ontologies.
What is the name and location of the building that a particular parking space serve?	This has been met through the implementation of the Building class, hasConstituent object property. This is provided by existing CUSP ontologies however a new parking space class was created.
Who are the organisations that supply parking spaces to an actor?	This has been met through the implementation of the Parking Space class, hasOrganisationOwner object property in the Smart Parking ontologies. This is provided by existing CUSP ontologies however a new parking space class was created.
How many parking spaces does a given building have?	This has been met through the implementation of the Parking Space class and its isConstituentOf object property in the Smart Parking ontology.
What sensor devices monitor a given parking space?	This has been met through the implementation of the Parking Space class and its hasSensor object property in the Smart Parking ontology.
What is the physical location of a given parking space?	This has been met through the implementation of the Space class and its isConstituentOf object property in CUSP ontology.
What is the total parking space capacity of given location?	This has been met through the implementation of the Parking Space class, isConstituentOf object relationship. Along with the hasConsitutent object property of the Building class.
What is the total free parking space capacity of given location at a given time?	This has been met through the implementation of the Parking Space class, isConstituentOf object property in the Smart Parking

	ontologies. There are 55 parking space at CU case study.
Is a particular parking space suitable for disabled users?	This has been met through the implementation of the Space class, This class has the following data properties; (parking space type) These have been added to the Smart Parking Management ontologies
What is information is held about a given student?	This has been met through the implementation of the Student class (subclass of actor). This class has the following data properties; First name, Last name, Email and phone Number Data. These have been added to the social ontology.
What is information is held about a given staff member?	This has been met through the implementation of the Staff Member class (subclass of Actor). This class has the following data properties; First name, Last name, Email and phone Number.
What is information is held about a given parking officer?	This has been met through the implementation of the Officer class (subclass of Actor). This class has the following data properties; First name, Last name, Email and phone Number.
What are the details of the service that manages smart parking system at a given location?	This has been met through the implementation of the Parking Space class, and the hasService object property that links it to the service that manages the parking space.
Identify all the smart parking services that require authentication?	This has been met through the implementation of the Smart Parking Service class, AssociatedWithResource Displaying University Parking Violation Service object property in the Service ontologies.

What parking violations have been issued to a given actor across all parking sites?	This has been met through the implementation of the Violation class, and the IssuedTo object property that connects violations and Actors
How many violations has a given parking officer issued and at what sites?	This has been met through the implementation of the Violation class, and the IssuedTo object property that connections violations and Officers.
What are is number of uses per day of a given parking space and their timestamps?	This has been met through the implementation of the Parking Space class, and the hasService object property to associate it to a Parking Service. Once processing of a reservation is complete the parking service records the number of uses using the numbeOfUses data property and records the timestamps using the useTimestamp data property.
Who are actors that administer a given parking space?	These have been implemented through the use of the Policy, Actor, Role, Permission, and Resource Classes. These classes allow the definition of a set of flexible permissions. An actor is (optionally) assigned to a role. At the same time resources (services or physical devices) provide. permissions that conceptualise what functionality that they can perform. Then a policy provides a mapping between user/role and permissions for a given resource.
Which actors can utilise a given parking space?	
Does a given actor have access to a book a parking space?	
What are the access control policies governing reservation on a parking space service?	
What are the access control policies governing the issue of violations on a parking space service?	
What are the access control policies to displaying the violations for a given parking space service?	

6.4 Instantiated access management ontology

This section illustrates the instantiated ontology that has been created. Figure 6.2 illustrates the smart systems classes (Smart Parking, Attendance Management System, Access Door System and Smart Air Conditioning System) that have been created and deployed.

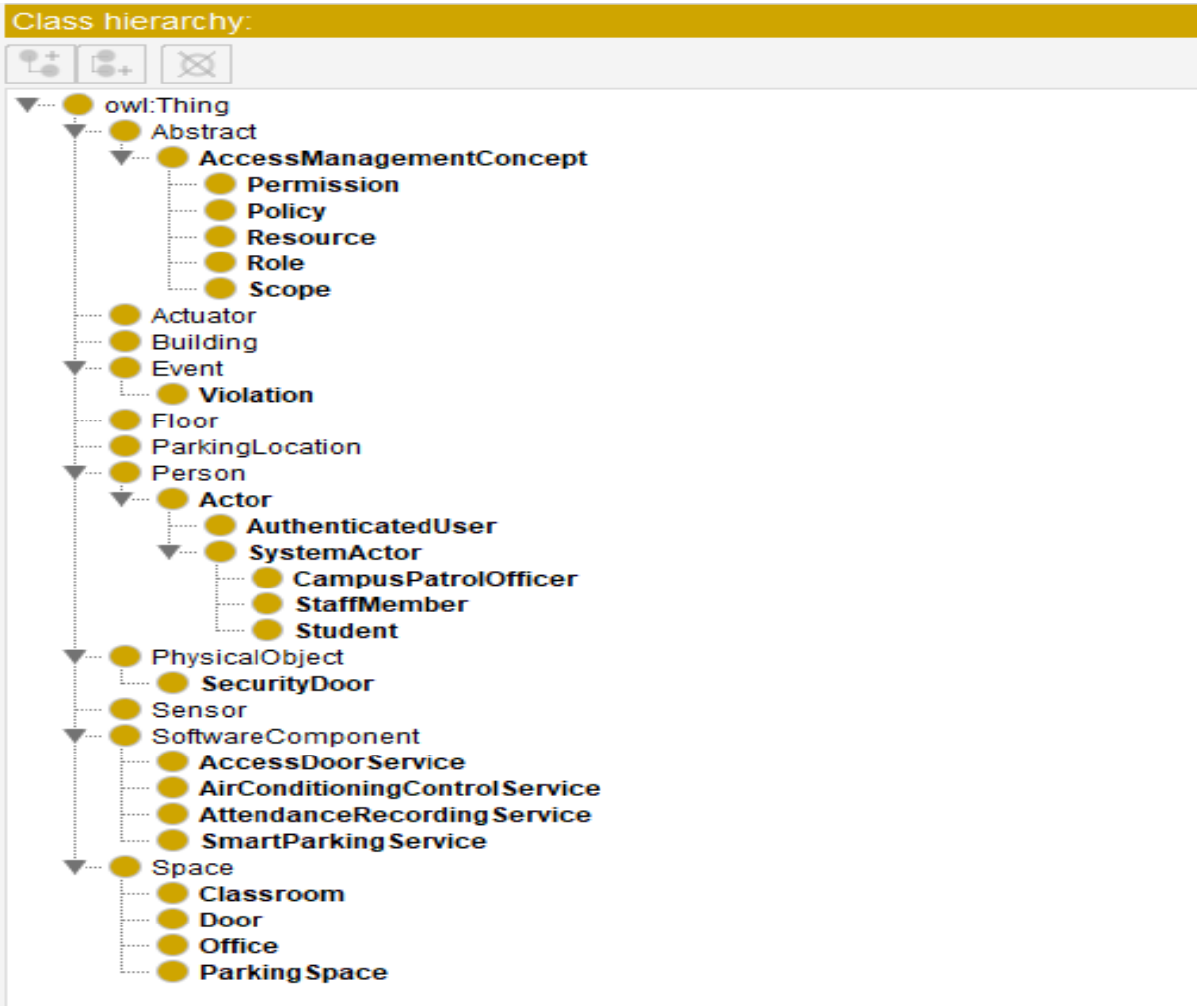


Figure 6.2 CU Smart Systems Classes

6.5 Verification & Validation on a university building case study

Previously, Chapter 5 identified the specification of an access management framework to overcome the access management research gaps (identified in….) for building environment use cases. Moreover, it focused on developing the semantically specified access management framework. Following the verification of the competency questions, the ontology will now be validated on the Cardiff University use case already deployed within the CUSP platform.

As described previously, this process consists of the following:

1. The ontologies developed in Chapter 5 are instantiated and integrated within the CUSP platform. A simple modification to the CUSP platform code will enable security decisions to be made based on the ontology.
2. The ontology will be validated to ensure it can adequately represent the security requirements of the selected CUSP use case.
3. The ontology will be validated to ensure it correctly functions in assigning and provisioning access rights to built environment services.

This approach goes beyond authentication into enabling the granting of specific authorisations to users. Associating digital identities (authentication) with access control policies applied to different services, all linked to physical assets.

In the case of this use case all users are either staff/students of Cardiff University. However, in reality user interacting with a digital twin may be from any organisation and are authenticated via their own identity providers using single sign on.

The Cardiff University use case currently deployed within the CUSP platform considers the following aspects of university management:

Smart Parking System: enables Cardiff University students and staff members to reserve parking and display the violation recorded by Campus Police Officers.

Attendance Management System: enables Cardiff University students to record their attendance.

Access Door System: Enables the management of access to secure doors for Cardiff University staff and students.

Smart Air Conditioning System: enables Cardiff University staff members to control the air conditioning in their university office space.

In the remainder of this section, the instantiated ontology is described, and the results of the verification & validation process are presented.

6.5.1 Verification &Validation of the instantiated access management ontology

This section shows the key elements that exist in the new ontology for the Cardiff University case study (Smart Parking system access control, Attendance Management System access control, Access Door System access control and Smart Conditioning System access control). Table 6.2 provides the social information that presents Cardiff University users of the Smart

Parking services; Table 6.3 shows the service information that presents the Smart System services at Cardiff University; Table 6.4 provides the sensor information that presents the sensor device used in Cardiff University's Smart System; Table 6.5 concerns access management and presents the policies applied in Cardiff University's Smart System.

Table 6.2 Cardiff University users who utilise the Smart System university services

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

Table 6.3 Smart System services at Cardiff University

Services	**Service Description**	**Physical Assets Managed**
University Parking Reservation Service	Available spaces at Queen Building, CU for Student and StaffMember	Parking Space at Queens' Building
Recording Of University Parking Violation Service	Recording the parking penalty by Campus police officer	Parking Space at Queen's Building

Displaying University Parking Violation Service	Displaying Parking Violation Service recorded for Student and StaffMember.	Parking Space at Queen's Building
Attendance Management Service	Student Attendance Recording at Classroom Queen Building, CU	Various Classrooms within Queen's Buildings
Access University Door Service	Access University Door atDoor Queen Building, CU	Various Doors in Queens' Buildings
Air Conditioning Control Service	Air Conditioning Control at Office Queen Building, CU	Various Offices at Queen's Building

Table 6.4 Sensor devices used in Cardiff University's Smart System

Sensor Device	**Physical Assets Connected to**
Parking Sensors	Record Parking Space at Queen Building, CU
Classroom Sensors	Record student attendance in Classroom at Queen Building, CU
Door Sensor	Record Access Door at Queen Building, CU
Office Sensor	Record Air Conditioning in Office at Queen Building, CU

Table 6.5 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 to Reserve University Parking	Allow if Role= “Student”	Make reservation	Reserve Parking Space
Allow Student to Displaying University Parking Violation	Allow if Role= “Student”	Display Violation	Display Violation
Allow Student Attendance Recording	Allow if Role= “Student”	Attendance Management	Attendance Management
Allow Student to Access University Door	Allow if Role= “Student”	Access University Door	Access University Door
Allow StaffMember to Access University Door	Allow if Role= “StaffMember”	Access University Door	Access University Door
Allow Staff to Air Conditioning Control	Allow if Role= “StaffMember,	Contro the Air Conditioning l	Air Conditioning Control

Finally, Table 6.6 summarises the overall verification & 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, Access University Doors, Attendance Recording and Air Conditioning Control (see Section 6.4). Therefore, the results in Table 6.6. show the ontology is functioning as expected.

Table 6.6 Access management ontology

Users	Reserve Parking Space	Record Parking Violation	Display Parking Violation	attendance recorded	Access Secure Door	Control Air Conditioning
Ahmed	Yes, user is granted access	No, user isn't granted access	Yes, user is granted access	No, user isn't granted access	Yes, user is granted access	Yes, user is granted access
Sara	Yes, user is granted access	No, user isn't granted access	Yes, user is granted access	Yes, user is granted access	Yes, user is granted access	No, user isn't 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	No, user isn't 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	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	No, user isn't granted access	No, user isn't granted access

6.6 Summary

From the perspective of creating a built-environment access management framework that fully utilises sensor networks, semantic web technologies have a long history of development and a strong community demonstrating how they can contribute to the development of interoperable systems in the real world. In fact, ontologies are semantic models of real-world

concepts that allow machines to comprehend data beyond their simple syntax. The purpose of the developed ontology is to integrate disparate semantics across the multiple domains involved (i.e. IoT Devices and cyber-physical systems, existing built environment services, existing security standards, digital twin, and BIM datasets as well as newly developed user interfaces and the actors who use them.). The proposed access management framework for digital twins in the built environment will be validated because of this.

This chapter has validated the Semantically Specified Access Management Framework, presenting the verification & validation methodology. This has showed the technical verification against Competency Questions and validated the ontology on a University Building Case Study deployed within the CUSP platform.

Overall, the evidence presented in this chapter has helped to fully answer the following research question:

RQ4: Can the current security processes employed by CPS and digital twins be improved to address the access management requirements of digital twins in the context of the built environment?

This RQ has been answered through the development and subsequent verification & validation of the access management ontology for digital twins in built environment as below:

- Performing a technical verification against competency questions: all competency questions were validated against the constructed ontology to ensure that the ontology answered them all. This shows that the ontology meets the requirement specification outlined in Chapter 5
- Performing a verification &validation by applying the ontology to a use case deployed on the Cardiff University CUSP Platform. To conduct this element of the validation, the access management ontology was integrated into the existing CUSP platform and tested on various case studies. This shows that the ontology correctly functions in a digital twin environment, providing appropriate access control and enabling single sign on.

Chapter 7: Conclusion and recommendations

This chapter recaps the motivation for the research and summary of the research conducted and summarises the key findings of this thesis and how this has addressed the research questions and hypothesis presented in Chapter 1. This chapter also summarises the main limitations and makes a several recommendations for future research.

7.1 Summary of contributions and the key findings

The contributions are summarised as follows:

- **Elicitation and description of the challenges and opportunities presented by digital twins in the built environment**. These challenges focused on the need for enhancement of existing access management practices in the built environment. This entailed reviewing the latest technology in the fields of BIM, the IoT, digital twins, smart cities, and access management as well as surveying industry attitudes to access management in the built environment and the obstacles to the further development of this area (see Chapter 2).
- **Development of a semantically specified access management framework for digital twins based on current industry standards:** This framework was developed through requirements engineering and subsequent ontological modelling process. This process explicitly expresses domain information and saves time and money during the development stage. It addressed built environment case studies, requirement specification, competency questions, analysis of existing ontological resources, built environment resources, re-engineering of built environment non-ontological resources, class diagrams and access management ontology. The ontology reflects the semantic integration required to achieve access management between physical built environment assets, IoT devices, cyber-physical systems, current built environment services, existing security standards, digital twin and BIM datasets, as well as newly developed user interfaces and the actors who use them. (See Chapter 5).
- **Enhancement of BIM standards to support the required access management concepts:** The developed ontology enables the formal provision of a security framework to deal with security risks that affect asset information and data. The ontology makes it possible to link with existing standards of ISO 19650-5:2020, i.e., by implementing access controls. The ontology also enables the integration with ifcOWL, and thus enables formalised semantic integration between physical built environment assets, IoT devices and cyber-physical systems (see Appendix G).

The key findings are summarised as follows:

- **Identification of current access management procedures, difficulties, and requirements for digital twins in the built environment**. This was performed using a literature review and industry survey for built environment experts from various organisations. The findings of the industry survey indicated that most organisations lack the tools and practises necessary to identify and prevent sensitive data from leaving digital twins/CPSs. In addition, the findings indicated that very few organisations had deployed digital twins in their projects (see Chapters 2 and 4).

- **Finding the semantically designed access management framework:** This involved deployment of the developed ontology within a digital twin platform (CUSP) and performing verification & validation on a university case study featuring various smart system services (Smart Parking System, Attendance Management System, Access Door System, Smart Air Conditioning System), demonstrating that the ontology functions correctly in providing access control capability across the multiple domains that it considers.

7.2 Research questions & hypothesis

The research questions were as follows:

RQ1: *How suitable are the current IoT and CPS security systems for providing access management for digital twins in the context of smart buildings and districts?*

RQ2: *What are the current obstacles to tackling access management threats to the built environment CPSs?*

RQ3: *What are the key requirements for a semantically specified access management framework suitable for the built environment?*

RQ4: *Can the current security processes employed by CPS and digital twins be improved to address the access management requirements of digital twins in the context of the built environment?*

The research hypothesis is as follows:

The introduction of a built-environment access management framework adapted to new technological advances will ensure the security and interoperability of built environment digital twins with existing ICT systems in common use today.

RQ1 was answered in Chapter 2: Here it was shown that current IoT and CPS security systems are not suitable for addressing access management threats twins in the context of smart buildings and districts.

This chapter discussed the digital twins, CPSs and BIM, revealing the associated shortcomings and the paucity of operative applications. Also in this chapter, smart cities and other current applications in the built environment were reviewed to illustrate the ongoing efforts in the domain. The key contribution of authentication and the authorisation process was then presented in smart city applications, as well as advising how to improve standardisation to enhance the domain's access management and ensure that future secure smart cities can incorporate digital twin and city standards.

RQ2 was answered in Chapter 4: Here it was shown that current obstacles to tackling access management threats to the built environment CPSs are; (a) cost and difficulty of adopting cyber security; (b) the tools and processes needed to identify and prevent the loss of sensitive data; (c) the ability to monitor DTs/CPSs to detect anomalous activities; (d) the lack of a single, established standard because each platform specifies its own protocols, encodings and APIs; and (e) the fact that the data needed for digital twins often is not in the hands of a single owner but spread across numerous stakeholders.

This chapter presented the industry survey that covered: (a) understanding the adoption of cyber-physical systems regarding the built environment; (b) understanding the adoption of digital twins in the built environment; (c) determining obstacles to the adoption of access management for digital twins/CPS in the built environment.

RQ3 was answered in Chapter 5: Here the key requirements for a semantically specified *access management* framework suitable for the built environment were formally documented.

This chapter focused on specifying and then creating the semantically specified *access management* framework by:

- Creating a semantically defined access management framework for the built environment.
- Formally specifying the key elements of the framework through ontological modelling.

RQ4 was answered in Chapter 6: Here it was shown that current security processes employed by CPS and digital twins can be improved to address the access management threats facing digital twins in the context of the built environment domain. This has been show through a rigorous verification & validation exercise.

This chapter identified the specification of an access management framework to overcome the access management research gaps (identified in …) for built environments utilising Cardiff University as a use case. It focused on developing the semantically specified access management framework that included testing that it was compatible with the required concepts for the built environment such as SSO. This phase of the research addressed the fourth research question so that an answer could be arrived at.

The answer to the hypothesis is that:

Access management frameworks can be applied for digital twins in the built environment, providing access control, data confidentiality and integrity, and single sign-on (SSO) across built-environment services leveraging digital twins, BIM data, and IoT. This thesis has shown that this can ensure the security and interoperability of built environment digital twins with existing ICT systems in common use today through the specification and subsequent verification & validation of an access management framework for digital twins in the built environment which is supported by the formal specification of a access management ontology. Through this specification of the ontology, a formal representation of domain information linked with access management concepts drawn from industry standards has been developed and subsequently validated using a case study in the built environment.

7.3 Study limitations

The research limitations are as follows:

Limitation 1: Access management research for digital twin technology is a new area of study within the built environment domain. As a result, experts in the built environment have differing perspectives and understandings of it. This is exacerbated by the limited number of experts in this area and the fact that organisations in the industry are often hesitant to share information about their procedures and operations. Thus, answers gathered regarding the need for and use of access management for digital twin technology in the building sector are typically varied and subjective, based on the experts' backgrounds. This was overcome by using a systematic multi-phase research approach (literature review, industry survey, eliciting obstacles and defining the access management framework, ontology development and verification

&validation) to reduce the effects of differing expert opinions on the use of access management for digital twin technology in the built environment.

Limitation 2: The lack of accessible real world use cases prevents direct observation of access management issues. As a result, an industry survey was utilised to identify gaps and allow the completion of numerous critical actions during the case study development process.

Limitation 3: The case study was a desk-based study with actual ontologies developed and their use simulated. However, this may not be sufficient to thoroughly test the case study's functionality. As a result, it is strongly advised that a live trial be developed on a real built environment asset.

7.4 Recommendations for future work

The current study identifies future research areas with the goal of further developing access management frameworks for digital twins in the built environment as follows:

Recommendation 1: Widen the consultation to include other built environment experts to further validate the ontology against other obstacles facing the rapidly evolving field of digital twins.

Recommendation 2: The testing and validation of the ontology is based on the validation of the ontology based on a case study in Cardiff University. In future, the ontology should be further validated on further real digital twin deployments outside of a controlled university setting. This is needed to fully ensure that the final outputs from the platform are secure and reliable.

Recommendation 3: Evaluate and test the developed access management framework on a wider variety of case studies to validate the ontology that has already been done in this thesis.

Recommendation 4: Further showcase the potential of the access management ontology through the development of new software tools to allow secure and scalable sharing of data between digital twins and digital twin operators. This will be required to allow the multiple digital twins that will be required to represent the future smart cities to share data adequately and securely.

7.5 Summary

This chapter has emphasised the motivation for the current research, namely the access management issue for digital twins in the built environment, and the recommendations for future work (see Section 7.5).

Access management is an essential component of the policies, architecture and operations of companies that work in the built environment. The willingness to address access management issues in a positive manner is a major concern for all parties. Furthermore, access management strategies should be fully integrated with organisational and IT strategies to maximise the overall efficiency of the actual output.

The current research has addressed problems by specifying a access management framework for digital twins in the built environment, providing guidance for the implementation of access controls, data confidentiality, integrity and SSO across built environment services, leveraging digital twin and BIM data. This has been underpinned by the formal specification of an access management ontology for digital twins in the built environment. Through this specification, a formal representation of domain information has been developed and subsequently validated using a case study in the built environment.

References

Aagesen, G. and Krogstie, J. (2010) 'Handbook on Business Process Management 1', *Handbook on Business Process Management 1*, (June 2014). doi: 10.1007/978-3-642-00416-2.

ABAB (2019) 'Australian BIM Strategic Framework', *Australasian BIM advisory board,* p. 18. Available at: http://www.abab.net.au/.

Abanda, F. H., Tah, J. H. M. and Keivani, R. (2013) 'Expert Systems with Applications Trends in built environment semantic Web applications : Where are we today ?', *Expert Systems With Applications*, 40(14), pp. 5563–5577. doi: 10.1016/j.eswa.2013.04.027.

Ademci, E. and Gundes, S. (2018) 'Review of Studies on BIM Adoption in AEC Industry Barriers to BIM Implementation', *Ademci, E., Gundes, S. (2018) Review of Studies on BIM Adoption in AEC Industry, 5th International Project and Construction Management Conference (IPCMC) Proceedings,* pp. 1046–1055.

Akbarieh, A. *et al.* (2020) 'BIM-based end-of-lifecycle decision making and digital deconstruction: Literature review', *Sustainability (Switzerland)*, 12(7). doi: 10.3390/su12072670.

Alam, M. I., Halder, R. and Pinto, J. S. (2021) 'A deductive reasoning approach for database applications using verification conditions', *Journal of Systems and Software*, 175. doi: 10.1016/j.jss.2020.110903.

Alameda, J. (2017) 'Extensible Markup Language', *Hydroinformatics*, (Xml), pp. 177–216. doi: 10.1201/9781420038002.ch11.

Alharahsheh, H. H. and Pius, A. (2020) 'A Review of key paradigms: positivism VS interpretivism', *Global Academic Journal of Humanities and Social Sciences*, 2(3), pp. 39–43. Available at: https://www.researchgate.net/publication/338244145.

Alshammari, K., Li, H. and Kwan, A. (2019) 'Security model collaborative building design'. *Proceedings of the 36th International Conference of CIB W78, Newcastle-upon-Tyne, UK,* 18-20 September, pp. 724-732 (ISSN: 2706-6568).

Alshammari, K., Beach, T. and Rezgui, Y. (2021a) 'Cybersecurity for digital twins in the built environment: Current research and future directions', *Journal of Information Technology in Construction*, 26(5), pp. 159–173. doi: 10.36680/j.itcon.2021.010.

Alshammari, K., Beach, T. and Rezgui, Y. (2021b) 'Industry Engagement for Identification of Cybersecurity Needs Practices for Digital Twins', *2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, pp. 1–7. doi: 10.1109/ice/itmc52061.2021.9570208.

Ameri, F. and Patil, L. (2012) 'Digital manufacturing market: a semantic web-based framework for agile supply chain deployment', *Journal of Intelligent Manufacturing,* pp. 1817–1832. doi: 10.1007/s10845-010-0495-z.

Arfi, W. Ben *et al.* (2021) 'The role of trust in intention to use the IoT in eHealth: Application of the modified UTAUT in a consumer context', *Technological Forecasting and Social Change*, 167(February), p. 120688. doi: 10.1016/j.techfore.2021.120688.

Arthur, S., Li, H. and Lark, R. (2017) 'A collaborative unified computing platform for building information modelling (BIM)', *IFIP Advances in Information and Communication Technology*, 506, pp. 63–73. doi: 10.1007/978-3-319-65151-4_6.

Arunkumar, S., Suveetha, V. and Ramesh, A. (2018) 'A feasibility study on the implementation of building information modeling (BIM): from the architects' & engineers' perspective', *Asian Journal of Civil Engineering*, 19(2), pp. 239–247. doi: 10.1007/s42107-018-0020-9.

Au, C. N. *et al.* (2021) 'A web-oriented architecture for deploying multiple unmanned vehicles as a service', *TransNav*, 15(1), pp. 155–162. doi: 10.12716/1001.15.01.15.

Autodesk (2003) 'Building Information Modeling for Sustainable Design', *Autodesk White Paper*, pp. 1–13.

Azorín, J. M. and Cameron, R. (2010) 'The application of mixed methods in organisational research: A literature review', *Electronic Journal of Business Research Methods*, 8(2), pp. 95–105.

Bada, M., Sasse, A. and Bada, M., Sasse, A., Nurse, J. (2019) 'Cyber Security Awareness Campaigns: Why They Fail to Change Behavior', *International Conference on Cyber Security for Sustainable Society*, p. 11. Available at: http://www.cs.ox.ac.uk/publications/publication9343-abstract.html%0Ahttp://discovery.ucl.ac.uk/1468954/1/Awareness CampaignsDraftWorkingPaper.pdf.

Baofu, H., Hui, L. and Chuansi, W. (2021) 'Blockchain-Based Distributed Data Integrity Auditing Scheme', *2021 IEEE 6th International Conference on Big Data Analytics, ICBDA 2021*, pp. 143–149. doi: 10.1109/ICBDA51983.2021.9403079.

Baonza, M. D. F., Pérez, A. and Villazón, B. (2010) 'NeOn Methodology for Building Ontology Networks: Specification, Scheduling and Reuse', *Methodology*, (February), pp. 1–18. Available at: http://kmi.open.ac.uk/events/sssw08/presentations/Gomez Perez-NeOn-Methodology-OntologySpecification-v3.pdf.

Barlish, K. (2011) 'How to Measure the Benefits of BIM', *Automation in Construction*, pp. 149–159.

Baškarada, S. and Koronios, A. (2018) 'A philosophical discussion of qualitative, quantitative, and mixed methods research in social science', *Qualitative Research Journal*, 18(1), pp. 2–21. doi: 10.1108/QRJ-D-17-00042.

Beach, T. H. *et al.* (2013) 'Cloud computing for the architecture, engineering & construction sector: Requirements, prototype & experience', *Journal of Cloud Computing*, 2(1), pp. 1–16. doi: 10.1186/2192-113X-2-8.

Bechhofer, S. (2004) 'OWL: Web Ontology Language', *Encyclopedia of Database Systems*, pp. 2640–2641. doi: 10.1007/978-1-4614-8265-9_1073.

Beetham, I. F. *et al.* (2014) 'Stakeholder perspectives on the value of car parking', *Urban, Planning and Transport Research*, 2(1), pp. 195–214. doi: 10.1080/21650020.2014.885385.

Bell, E., Bryman, A. and Harley, B. (2017) 'Business research methods', *Oxford university press,* ISBN: 0198809875, 9780198809876.

Beltran, V. and Bertin, E. (2015) 'Identity management for Web business communications', *2015 18th International Conference on Intelligence in Next Generation Networks, ICIN 2015*, pp. 103–107. doi: 10.1109/ICIN.2015.7073814.

Bendraou, R. *et al.* (2010) 'A comparison of six UML-based languages for software process modeling', *IEEE Transactions on Software Engineering*, 36(5), pp. 662–675. doi: 10.1109/TSE.2009.85.

Beniaminov, E. M. (2018) 'Ontology Libraries on the Web: Status and Prospects', *Automatic Documentation and Mathematical Linguistics*, 52(3), pp. 117–120. doi: 10.3103/s0005105518030020.

Berners-Lee, T. (1989) 'Information Management: A Proposal. Internal Project Proposal', *Cern*, (May), p. 20. Available at: https://cds.cern.ch/record/369245/files/dd-89-001.pdf.

BIMGroup (2011) 'A report for the Government Construction Client Group Building Information Modelling (BIM) Working Party Strategy Paper', (March). Available at:

https://www.cdbb.cam.ac.uk/Resources/ResoucePublications/BISBIMstrategyReport.pdf.

Blasch, E. (2015) 'Ontologies for nextgen avionics systems', *AIAA/IEEE Digital Avionics Systems Conference - Proceedings*, (September 2015), p. 3B51-3B513. doi: 10.1109/DASC.2015.7311395.

Blosch, M. (2001) 'Pragmatism and organizational knowledge management', *Knowledge and Process Management*, 8(1), pp. 39–47. doi: 10.1002/kpm.95.

Bodenreider, O. and Stevens, R. (2006) 'Bio-ontologies: current trends and future directions', *Briefings in bioinformatics*, 7(3), pp. 256–274. doi: 10.1093/bib/bbl027.

Boje, C., Bolshakova, V., *et al.* (2020) 'Semantics for linking data from 4D BIM to digital collaborative support', *Frontiers of Engineering Management*. doi: 10.1007/s42524-020-0111-7.

Boje, C., Guerriero, A., *et al.* (2020) 'Towards a semantic Construction Digital Twin: Directions for future research', *Automation in Construction*, 114(March), p. 103179. doi: 10.1016/j.autcon.2020.103179.

Bolton A, Enzer M, S. J. et al. (2018) 'The Gemini Principles', *Centre for Digital Built Britain: University of Cambridge*, p. 15. Available at: https://www.cdbb.cam.ac.uk/system/files/documents/TheGeminiPrinciples.pdf.

Bore, N. *et al.* (2020) 'AGWS: Blockchain-enabled Small-scale Farm Digitization', *IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2020*. doi: 10.1109/ICBC48266.2020.9169450.

Borgia, E. (2014) 'The internet of things vision: Key features, applications and open issues', *Computer Communications*, 54, pp. 1–31. doi: 10.1016/j.comcom.2014.09.008.

Bosch, A., Volker, L. and Koutamanis, A. (2015) 'BIM in the operations stage: bottlenecks and implications for owners', *Built Environment Project and Asset Management*, 5(3), pp. 331–343. doi: 10.1108/BEPAM-03-2014-0017.

El Bousty, H. *et al.* (2018) 'Investigating business intelligence in the era of big data: Concepts, benefits and challenges', *ACM International Conference Proceeding Series*, (March). doi: 10.1145/3234698.3234723.

Boyes, H. (2014) 'Building Information Modelling (BIM): Addressing the Cyber Security Issues', *IET The Institution of Engineering and Technology*, pp. 1–12. doi: 10.1049/etr.2014.9001.

Boyes, H. (2015) 'security, privacy and the Built Environment', *IT Professional*, 17, pp. 25–31. doi: 10.1109/MITP.2015.49.

Bryde, D., Broquetas, M. and Volm, J. M. (2013) 'The project benefits of building information modelling (BIM)', *International Journal of Project Management*, 31(7), pp. 971–980. doi: 10.1016/j.ijproman.2012.12.001.

BSI (2007) 'BS 1192-2007 +A1-2015_Collaborative production of architectural , engineering and construction information - Code of practice', *BSI*, (2015), p. 40.

Burov, Y., Mykich, K. and Karpov, I. (2021) 'Intelligent Systems Based on Ontology Representation Transformations', *Conference on Computer Science and Information Technologies*, pp. 263–275. doi: 10.1007/978-3-030-63270-0_18.

C Eastman, P Teicholtz, R. S. and K. L. (2011) *BIM Handbook: A Guide to Building Information Modeling for Owners, Managers, Designers, Engineers and Contractors*, *Anthropology & Medicine*. doi: 10.1080/13648470.2013.812871.

Cains, M. G. *et al.* (2021) 'Defining Cyber Security and Cyber Security Risk within a Multidisciplinary

Context using Expert Elicitation', *Risk Analysis*. doi: 10.1111/risa.13687.

Candidate, D. D., Kelly, G. and Kassem, P. M. (2021) 'BIM , DIGITAL TWIN AND CYBER-PHYSICAL SYSTEMS : CROSSING AND BLURRING BOUNDARIES Northumbria University , Newcastle-Upon-Tyne , UK BIM Academy , Newcastle Upon Tyne , United Kingdom', (3).

Canli, H. and Toklu, S. (2021) 'Deep Learning-Based Mobile Application Design for Smart Parking', *IEEE Access*, 9, pp. 61171–61183. doi: 10.1109/ACCESS.2021.3074887.

Car, N. *et al.* (2018) 'netCDF-LD SKOS: Demonstrating Linked Data Vocabulary Use Within netCDF-Compliant Files', *International Symposium on Environmental Software Systems,* pp. 329-337.

Cardullo, P. and Kitchin, R. (2019) 'Smart urbanism and smart citizenship: The neoliberal logic of "citizen-focused" smart cities in Europe', *Environment and Planning C: Politics and Space*, 37(5), pp. 813–830. doi: 10.1177/0263774X18806508.

Carroll, J. *et al.* (2011) 'OWL: Web Ontology Language', *W3C*, pp. 1–53. doi: 10.1007/springerreference_64035.

Çelik, A. *et al.* (2018) 'Social Research Methods', *Journal of Materials Processing Technology*, 1(1), pp. 1–8. Available at: http://dx.doi.org/10.1016/j.cirp.2016.06.001%0Ahttp://dx.doi.org/10.1016/j.powtec.2016.12.055%0Ahttps://doi.org/10.1016/j.ijfatigue.2019.02.006%0Ahttps://doi.org/10.1016/j.matlet.2019.04.024%0Ahttps://doi.org/10.1016/j.matlet.2019.127252%0Ahttp://dx.doi.o.

Cha, H. S. and Lee, D. G. (2015) 'A case study of time/cost analysis for aged-housing renovation using a pre-made BIM database structure', *KSCE Journal of Civil Engineering*, 19(4), pp. 841–852. doi: 10.1007/s12205-013-0617-1.

Chan, D. W. M., Olawumi, T. O. and Ho, A. M. L. (2019) 'Perceived benefits of and barriers to Building Information Modelling (BIM) implementation in construction: The case of Hong Kong', *Journal of Building Engineering*, 25(8), p. 100764. doi: 10.1016/j.jobe.2019.100764.

Chen, E. *et al.* (2014) 'OAuth demystified for mobile application developers', *Proceedings of the ACM Conference on Computer and Communications Security*, (1), pp. 892–903. doi: 10.1145/2660267.2660323.

Chen, M. *et al.* (2016) 'Smart Clothing: Connecting Human with Clouds and Big Data for Sustainable Health Monitoring', *Mobile Networks and Applications*, 21(5), pp. 825–845. doi: 10.1007/s11036-016-0745-1.

Chimay, R.-E. (2020) 'Cyber-Physical Systems in the Built Environment', *Springer International Publishing*. doi: 10.1007/978-3-030-41560-0.

Chourabi, H. *et al.* (2012) 'Understanding smart cities: An integrative framework', *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 2289–2297. doi: 10.1109/HICSS.2012.615.

Chuang, T. H., Lee, B. C. and Wu, I. C. (2011) 'Applying cloud computing technology to BIM visualization and manipulation', *Proceedings of the 28th International Symposium on Automation and Robotics in Construction, ISARC 2011*, (June 2011), pp. 144–149. doi: 10.22260/isarc2011/0023.

Chun, S. *et al.* (2020) 'Designing an integrated knowledge graph for smart energy services', *Journal of Supercomputing*, 76(10), pp. 8058–8085. doi: 10.1007/s11227-018-2672-3.

Ciberseguridad, O. E. N. (2021) 'Cybersecurity Ontologies : A Systematic Literature Review', *ReCIBE, Revista electrónica de Computación, Informática, Biomédica y Electrónica*, *9* (2), pp. 1–18.

Cisco (2014) 'The Internet of Things Reference Model', *Internet of Things World Forum, white paper*, pp. 1–12.

Cooper, D. R. and Schindler, P. S. (2014). Business Research Methods 12th Edition. *Business Research Methods*. McGraw Hill.

Corallo, A., Lazoi, M. and Lezzi, M. (2020) 'Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts', *Computers in Industry*, 114, p. 103165. doi: 10.1016/j.compind.2019.103165.

Corbetta, P. (2013) 'Social Research: Theory Methods and Techniques the Use of Documents', *SAGE.* doi: http://dx.doi.org/10.4135/9781849209922.n11.

Cox, S. J. D. (2017) 'Ontology for observations and sampling features, with alignments to existing models', *Semantic Web*, 8(3), pp. 453–470. doi: 10.3233/SW-160214.

Dang, H. B., Abramovici, M. and Go, J. C. (2016) 'CIRP Annals - Manufacturing Technology Semantic data management for the development and continuous reconfiguration of smart products and systems', *CIRP Annals,* 65(1), pp. 185–188.

Darif, A., Chaibi, H. and Saadane, R. (2019) 'Energy optimization of SWIMAC for WSN based on IR-UWB in smart cities by using network coding', *ACM International Conference Proceeding Series*, (April), pp. 3–8. doi: 10.1145/3368756.3369037.

Das, M., Cheng, J. C. and Kumar, S. S. (2015) 'Social BIMCloud: a distributed cloud-based BIM platform for object-based lifecycle information exchange', *Visualization in Engineering*, 3(1). doi: 10.1186/s40327-015-0022-6.

Das, M., Cheng, J. C. P. and Kumar, S. S. (2014) 'BIMCloud: A Distributed Cloud-based Scoial BIM Framework for Project Collaboration', *The 6th International ASCE Conference on Computing in Civil and Building Engineering*, pp. 41–48. doi: 10.1061/9780784413616.006.

Dastjerdi, A. V. *et al.* (2016) 'Fog Computing: Principles, architectures, and applications', *Internet of Things: Principles and Paradigms*, pp. 61–75. doi: 10.1016/B978-0-12-805395-9.00004-6.

Demertzis, K., Iliadis, L. S. and Anezakis, V. D. (2018) 'An innovative soft computing system for smart energy grids cybersecurity', *Advances in Building Energy Research*, 12(1), pp. 3–24. doi: 10.1080/17512549.2017.1325401.

Demirkan, H. (2013) 'A Smart Healthcare Systems Framework', *It Professional*, 15(5), pp.38-45.

Denise Polit and Tatano Beck (2013) *Essentials of Nursing Research: Appraising Evidence for Nursing Practice*, *AORN Journal*. doi: 10.1016/j.aorn.2011.10.009.

Dibley, M. *et al.* (2012) 'An ontology framework for intelligent sensor-based building monitoring', *Automation in Construction*, 28, pp. 1–14. doi: 10.1016/j.autcon.2012.05.018.

Ding, K. *et al.* (2018) 'Smart steel bridge construction enabled by BIM and Internet of Things in industry 4.0: A framework', *2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC)*, pp. 1–5. doi: 10.1109/ICNSC.2018.8361339.

Dirsumilli, R. and Mossakowski, T. (2016) 'RESTful encapsulation of OWL API', *DATA 2016 - Proceedings of the 5th International Conference on Data Management Technologies and Applications*, (Data), pp. 150–157. doi: 10.5220/0005987201500157.

Dodanduwa, K. and Kaluthanthri, I. (2018) 'Role of trust in oauth 2.0 and OpenID connect', *2018 IEEE International Conference on Information and Automation for Sustainability (ICIAfS),* pp. 1–4.

Donatella Della Porta, M. K. (2008) 'Approaches and methodologies in the social sciences: A pluralist perspective', *Cambridge University Press*, ISBN:0521883229, 978-0521883221.

Doumbouya, L., Gao, G. and Guan, C. (2016) 'Adoption of the Building Information Modeling (BIM) for Construction Project Effectiveness: The Review of BIM Benefits', *American Journal of Civil Engineering and Architecture*, 4(3), pp. 74–79. doi: 10.12691/ajcea-4-3-1.

Eadie, R. *et al.* (2014) 'Building Information Modelling Adoption: An Analysis of the Barriers to Implementation', *Journal of Engineering and Architecture*, 2(1), pp. 77–101. doi: 10.1007/s13398-014-0173-7.2.

Eckhart, M. and Ekelhart, A. (2018) 'Towards Security-Aware Virtual Environments for Digital Twins', *Proceedings of the 4th ACM workshop on cyber-physical system security,* pp. 61–72.

Effendi, Y. A. and Sarno, R. (2018) 'Implementation of the semantic web in business process modeling using Petri nets', *2018 International Conference on Information and Communications Technology, ICOIACT 2018*, 2018– January, pp. 741–746. doi: 10.1109/ICOIACT.2018.8350724.

Eisenhauer, J. *et al.* (2006) 'Roadmap to Secure Control Systems in the Energy Sector', *Energetics Incorporated. Sponsored by the US Department of Energy and the US Department of Homeland Security,* URL: Roadmap to Secure Control Systems in the Energy Sector.

Ekaputra, F. J. (2020) 'Semantics for Cyber-Physical Systems: A Cross-Domain Perspective', *Semantic Web*, 11(1), pp.115-124.

Enshassi, M. A., Al Hallaq, K. A. and Tayeh, B. A. (2019) 'Limitation Factors of Building Information Modeling (BIM) Implementation', *The Open Construction & Building Technology Journal*, 13(1), pp. 189–196. doi: 10.2174/1874836801913010189.

Eriksson, H.-E. and M. P. (2001) 'Business process modeling with UML', *ICEIS 2001 - Proceedings of the 3rd International Conference on Enterprise Information Systems*, 2, pp. 679–685.

Eschenauer, L. and Gligor, V. D. (2002) 'A Key-Management Scheme for Distributed Sensor Networks', *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 41–47.

Fazio, M. and Celesti, A. (2015) 'Exploiting the FIWARE Cloud Platform to Develop a Remote Patient Monitoring System', *2015 IEEE Symposium on Computers and Communication (ISCC),* pp. 264–270. doi: 10.1109/ISCC.2015.7405526.

Fugar, F. D. K. and Adinyira, E. (2019) '14 th INTERNATIONAL POSTGRADUATE RESEARCH CONFERENCE 2019 : Contemporary and Future Directions in the Built Environment', *Sustainable Construction and Sustainability Expertise - Underlying Concepts: Getting the Balance Right*, (December), pp. 396–403.

Generation, D. and Storage, E. (2011) *IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications , and Loads IEEE Standards Coordinating Committee 21 Sponsored by the*.

Gha, A. *et al.* (2017) 'Application of nD BIM Integrated Knowledge-based Building Management System (BIM-IKBMS) for inspecting post-construction energy efficiency', *Renewable and Sustainable Energy Reviews*, 72(2), pp. 935–949. doi: 10.1016/j.rser.2016.12.061.

Ghauri, P., Grønhaug, K. and Strange, R. (2020) 'Research Methods in Business Studies', *Research Methods in Business Studies*. doi: 10.1017/9781108762427.

Ginzburg, A. *et al.* (2016) 'Implementation of BIM-technologies in Russian construction industry according to the international experience', *Journal of Applied Engineering Science*, 14(4), pp. 457–460. doi: 10.5937/jaes14-12567.

Gollmann, D. (2019) 'Authorisation, Authorisation & Accountability (AAA) Knowledge Area Issue,' *Hamburg University of Technology & Nanyang Technological University Singapore,* pp. 1-38.

Górka, M. (2021) 'Cybersecurity Politics – Conceptualization of the Idea', *Polish Political Science Yearbook*, 50(1), pp. 71–89.

GRAY, D. E. (2018) 'Doing Research in the Real World', *Journal of Materials Processing Technology*, 1(1), pp. 1–8. Available at: http://dx.doi.org/10.1016/j.cirp.2016.06.001%0Ahttp://dx.doi.org/10.1016/j.powtec.2016.12.055%0Ahttps://doi.org/10.1016/j.ijfatigue.2019.02.006%0Ahttps://doi.org/10.1016/j.matlet.2019.04.024%0Ahttps://doi.org/10.1016/j.matlet.2019.127252%0Ahttp://dx.doi.o.

Gray, J. A., Zimmerman, J. L. and Rimmer, J. H. (2012) 'Built environment instruments for walkability, bikeability, and recreation: Disability and universal design relevant?', *Disability and Health Journal*, 5(2), pp. 87–101. doi: 10.1016/j.dhjo.2011.12.002.

Grieves, M. (2014) 'Digital Twin : Manufacturing Excellence through Virtual Factory Replication - A Whitepaper by Dr . Michael Grieves', *White Paper*, (March), pp. 1–7. [Online]. Available: http://innovate.fit.edu/plm/documents/doc_mgr/912/1411.0_Digital_Twin_White_Paper_Dr_Grieves.pdf.

Grilo, A. and Jardim-Goncalves, R. (2010) 'Value proposition on interoperability of BIM and collaborative working environments', *Automation in Construction*, 19(5), pp. 522–530. doi: 10.1016/j.autcon.2009.11.003.

Grilo, A. and Jardim-Goncalves, R. (2011) 'Challenging electronic procurement in the AEC sector: A BIM-based integrated perspective', *Automation in Construction*, 20(2), pp. 107–114. doi: 10.1016/j.autcon.2010.09.008.

Gubbi, J. *et al.* (2013) 'Internet of Things (IoT): A vision , architectural elements , and future directions', *Future Generation Computer Systems*, 29(7), pp. 1645–1660. doi: 10.1016/j.future.2013.01.010.

Guerriero, A. *et al.* (2017) 'BIM-enhanced Collaborative Smart Technologies for LEAN Construction Processes', *2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC),* pp. 1023–1030.

Gupta, M., Patwa, F. and Sandhu, R. (2018) 'An attribute-based access control model for secure big data processing in hadoop ecosystem', *ABAC 2018 - Proceedings of the 3rd ACM Workshop on Attribute-Based Access Control, Co-located with CODASPY 2018*, 2018–Janua, pp. 13–24. doi: 10.1145/3180457.3180463.

Gupta, M. and Sandhu, R. (2021) *Towards activity-centric access control for smart collaborative ecosystems*, *Proceedings of ACM Symposium on Access Control Models and Technologies, SACMAT*. Association for Computing Machinery. doi: 10.1145/3450569.3463559.

Gushev, M. (2020) 'Dew Computing Architecture for Cyber-Physical Systems and IoT', *Internet of Things*, 11, p. 100186. doi: 10.1016/j.iot.2020.100186.

Haag, S. and Anderl, R. (2018) 'Digital twin – Proof of concept', *Manufacturing letters*, pp. 64–66. doi: 10.1016/j.mfglet.2018.02.006.

Haller, A. *et al.* (2018) 'The modular SSN ontology: A joint W3C and OGC standard specifying the semantics of sensors, observations, sampling, and actuation', *Semantic Web*, 10(1), pp. 9–32. doi: 10.3233/SW-180320.

Hancke, G. P., de Silva, B. de C. and Hancke, G. P. (2013) 'The role of advanced sensing in smart cities',

Sensors (Switzerland). doi: 10.3390/s130100393.

Hashem, I. A. T. *et al.* (2016a) 'The role of big data in smart city', *International Journal of Information Management*, 36(5), pp. 748–758. doi: 10.1016/j.ijinfomgt.2016.05.002.

Hashem, I. A. T. *et al.* (2016b) 'The role of big data in smart city', *International Journal of Information Management*, 36(5), pp. 748–758. doi: 10.1016/j.ijinfomgt.2016.05.002.

Hashmi, M., Hänninen, S. and Mäki, K. (2011) 'Survey of smart grid concepts, architectures, and technological demonstrations worldwide', *2011 IEEE PES Conference on Innovative Smart Grid Technologies Latin America SGT LA 2011 - Conference Proceedings*, pp. 1–7. doi: 10.1109/ISGT-LA.2011.6083192.

Hassan, B. (2016) 'Towards Semantic Web: Challenges and Needs', *International Journal Of Engineering And Computer Science*, 4(10), pp. 4–7. doi: 10.18535/ijecs/v4i10.08.

Hines, T (2000) 'An evaluation of two qualitative methods (focus group interviews and cognitive maps) for conducting research into entrepreneurial decision making', *Qualitative Market Research: An International Journal*, 3(1), pp. 7–16.

Hippolyte, J. L. *et al.* (2018) 'Ontology-driven development of web services to support district energy applications', *Automation in Construction*, 86(9), pp. 210–225. doi: 10.1016/j.autcon.2017.10.004.

Hire, S., Sandbhor, S. and Ruikar, K. (2021) 'Bibliometric Survey for Adoption of Building Information Modeling (BIM) in Construction Industry– A Safety Perspective', *Archives of Computational Methods in Engineering*, (0123456789). doi: 10.1007/s11831-021-09584-9.

Hooper, M. and Ekholm, A. (2010) 'a Pilot Study: Towards Bim Integration - an Analysis of Design Information Exchange & Coordination', *Proceedings of the CIB W78 2010: 27th International Conference –Cairo, Egypt, 16-18 November*, p. 2010.

Hordijk, R. *et al.* (2019) 'Defining a framework for medical teachers' competencies to teach ethnic and cultural diversity: Results of a European Delphi study', *Medical Teacher*, 41(1), pp. 68–74. doi: 10.1080/0142159X.2018.1439160.

Horridge, M. and Musen, M. (2016) 'Snap-SPARQL: A java framework for working with SPARQL and OWL', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9557, pp. 154–165. doi: 10.1007/978-3-319-33245-1_16.

Hou, S. (2015) 'An ontology-based holistic approach for multi-objective sustainable structural design', (September), pp. 1–254. Available at: http://ezproxy.leedsbeckett.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsble&AN=edsble.685495&site=eds-live&scope=site.

Howard, R. (2008) 'Building information modelling – Experts' views on standardisation and industry deployment', *Advanced engineering informatics*, 22, pp. 271–280. doi: 10.1016/j.aei.2007.03.001.

Howell, S. *et al.* (2017) 'Towards the next generation of smart grids : Semantic and holonic multi- agent management of distributed energy resources', *Renewable and Sustainable Energy Reviews*, 77(March), pp. 193–214. doi: 10.1016/j.rser.2017.03.107.

Howell, S., Beach, T. and Rezgui, Y. (2021) 'Robust requirements gathering for ontologies in smart water systems', *Requirements Engineering*, 26(1), pp. 97–114. doi: 10.1007/s00766-020-00335-z.

Howell, S. and Rezgui, Y. (2018) 'Beyond BIM Knowledge management for a smarter future', *IHS Markit*, ISBN:978-1-84806-476-8.

Hu, V. C. *et al.* (2013) 'Guide to attribute based access control (abac) definition and considerations',

NIST Special Publication, 800, p. 162.

Huang, Y. *et al.* (2009) 'Understanding the physical and economic consequences of attacks on control systems', *International Journal of Critical Infrastructure Protection*, 2(3), pp. 73–83. doi: 10.1016/j.ijcip.2009.06.001.

Ijeri, D., Maidargi, P. and Sunagar, R. (2020) 'Traffic Control System Using Image Proccesing', *Proceedings of B-HTC 2020 - 1st IEEE Bangalore Humanitarian Technology Conference*. doi: 10.1109/B-HTC50970.2020.9298014.

Iqbal, K. *et al.* (2018) 'Intelligent transportation system (ITS) for smart-cities using Mamdani Fuzzy Inference System', *International Journal of Advanced Computer Science and Applications*, 9(2), pp. 94–105. doi: 10.14569/IJACSA.2018.090215.

Jalali, R., El-Khatib, K. and McGregor, C. (2015) 'Smart city architecture for community level services through the internet of things', *2015 18th International Conference on Intelligence in Next Generation Networks, ICIN 2015*, pp. 108–113. doi: 10.1109/ICIN.2015.7073815.

Jayasankar, T. *et al.* (2021) 'Securing Medical Data using Extended Role Based Access Control Model and Twofish Algorithms on Cloud Platform', *European Journal of Molecular & Clinical Medicine*, 08(01), pp. 1075–1089.

Jiang, L., Kuhn, W. and Yue, P. (2017) 'An interoperable approach for Sensor Web provenance', *2017 6th International Conference on Agro-Geoinformatics, Agro-Geoinformatics 2017*, (July 2018). doi: 10.1109/Agro-Geoinformatics.2017.8047046.

Jiang, X. *et al.* (2021) 'Enhancing IoT Security via Cancelable HD-sEMG-based Biometric Authentication Password, Encoded by Gesture', *IEEE Internet of Things Journal*, XX(X), pp. 1–12. doi: 10.1109/JIOT.2021.3074952.

Johnson, R. B. and Onwuegbuzie, Anthony J, L. A. (2007) 'Toward a Definition of Mixed Methods Research', *Journal of Mixed Methods Research*, 1(2), pp. 112–133. doi: 10.1177/1558689806298224.

Jung, M., Reinisch, C. and Kastner, W. (2012) 'Integrating Building Automation Systems and IPv6 in the Internet of Things', *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pp. 683–688. doi: 10.1109/IMIS.2012.134.

Kagermann, H., Wahlster, W. and Helbig, J. (2013) 'Recommendations for implementing the strategic', *Frankfurt: National Academy of Science and Engineering,* p. 82.

Kalfa, S. M. (2018) 'Building information modeling (BIM) systems and their applications in Turkey', *Journal of Construction Engineering, Management & Innovation*, 1(1), pp. 55–66. doi: 10.31462/jcemi.2018.01055066.

Karl Popper (2010) 'The logic of scientific discovery', *Central Works of Philosophy Volume 4: The Twentieth Century: Moore to Popper*. doi: 10.1017/UPO9781844653614.015.

Karlof, C. (2003) 'Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures' *Ad hoc networks*, *1*(2-3), pp.293-315.

Kassem, M. and Succar, B. (2017) 'Macro BIM adoption: Comparative market analysis', *Automation in Construction*, 81, pp. 286–299. doi: 10.1016/j.autcon.2017.04.005.

Kayan, H. *et al.* (2021) 'Cybersecurity of Industrial Cyber-Physical Systems: A Review', *ACM Computing Surveys (CSUR)*.

Khan, Z., Anjum, A. and Kiani, S. L. (2013) 'Cloud based big data analytics for smart future cities',

Proceedings - 2013 IEEE/ACM 6th International Conference on Utility and Cloud Computing, UCC 2013, pp. 381–386. doi: 10.1109/UCC.2013.77.

Khanna, A. and Anand, R. (2016) 'IoT based smart parking system', *2016 International Conference on Internet of Things and Applications, IOTA 2016*, pp. 266–270. doi: 10.1109/IOTA.2016.7562735.

Khudhair, A. *et al.* (2021) 'Towards future BIM technology innovations: A bibliometric analysis of the literature', *Applied Sciences (Switzerland)*, 11(3), pp. 1–21. doi: 10.3390/app11031232.

Kibria, M. G. *et al.* (2017) 'Web objects based energy efficiency for smart home IoT service provisioning', *International Conference on Ubiquitous and Future Networks, ICUFN*, pp. 55–60. doi: 10.1109/ICUFN.2017.7993747.

Kim, C., Kim, C. and Son, H. (2013) 'Automated construction progress measurement using a 4D building information model and 3D data', *Automation in Construction*, 31, pp. 75–82. doi: 10.1016/j.autcon.2012.11.041.

Kirstein, P. T. and Ruiz-zafra, A. (2016) 'Use of Templates and The Handle for Large-Scale Provision of Security and IoT in the Built Environment', *Living in the Internet of Things: Cybersecurity of the IoT-2018*, pp. 1–10.

Kuster, C., Hippolyte, J. L. and Rezgui, Y. (2018) 'Collaborative Network for District Energy Operation and Semantic Technologies: A Case Study', *IFIP Advances in Information and Communication Technology*, 534, pp. 486–495. doi: 10.1007/978-3-319-99127-6_42.

Kuster, C., Hippolyte, J. L. and Rezgui, Y. (2020) 'The UDSA ontology: An ontology to support real time urban sustainability assessment', *Advances in Engineering Software*, 140. doi: 10.1016/j.advengsoft.2019.102731.

Layouni, F. and Pollet, Y. (2009) 'An ontology-based architecture for federated identity management', *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, pp. 162–166. doi: 10.1109/AINA.2009.124.

Lehmann, J. *et al.* (2017) 'SPARQLES: Monitoring Public SPARQL Endpoints', *Semantic web*, 8(6), pp. 1–17.

Lehtinen, T. O. A. *et al.* (2014) 'Perceived causes of software project failures - An analysis of their relationships', *Information and Software Technology*, 56(6), pp. 623–643. doi: 10.1016/j.infsof.2014.01.015.

Lemlouma, T., Laborie, S. and Roose, P. (2013) 'Toward a context-aware and automatic evaluation of elderly dependency in smart homes and cities', *2013 IEEE 14th International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2013*. doi: 10.1109/WoWMoM.2013.6583501.

Lethbridge, T. C., Sim, S. E. and Singer, J. (2005) *Studying software engineers: Data collection techniques for software field studies*, *Empirical Software Engineering*. doi: 10.1007/s10664-005-1290-x.

Lezzi, M., Lazoi, M. and Corallo, A. (2018) 'Cybersecurity for Industry 4.0 in the current literature: A reference framework', *Computers in Industry*, 103, pp. 97–110. doi: 10.1016/j.compind.2018.09.004.

Li, W., Mitchell, C. J. and Chen, T. (2019) 'Oauthguard: Protecting user security and privacy with Oauth 2.0 and Openid connect', *Proceedings of the ACM Conference on Computer and Communications Security*, (2), pp. 35–44. doi: 10.1145/3338500.3360331.

Lincoln, Y. S. and Guba, E. G. (2011) 'Paradigmatic controversies, contradictions and emerging confluences', *The Sage handbook of qualitative research*, *4*(2), pp.97-128.

Lings, L. and (2008) 'What is research and why would anyone want to do it?', *Doing Business Research*, pp. 1–19.

List, B. and Korherr, B. (2006) 'An evaluation of conceptual business process modelling languages', *Proceedings of the ACM Symposium on Applied Computing*, 2(Section 3), pp. 1532–1539. doi: 10.1145/1141277.1141633.

Liu, F. *et al.* (2013) 'Building Knowledge Modeling: Integrating Knowledge in BIM, *Proceedings of the 30th International Conference of CIB W78*, (30), pp. 9–12.

Liu, M. *et al.* (2021) 'Review of digital twin about concepts, technologies, and industrial applications', *Journal of Manufacturing Systems*, 58(July), pp. 346–361. doi: 10.1016/j.jmsy.2020.06.017.

Luck, A. and Boyes, H., (2015) 'Introduction to PAS 1192-5: 2015 A specification for security-minded building information modelling, digital built environments and smart asset management Introduction', *British Standards Inst., PAS*, pp.1192-5.

Luk, M. *et al.* (2007) 'MiniSec: A Secure Sensor Network Communication Architecture', *2007 6th International Symposium on Information Processing in Sensor Networks,* pp. 479–488.

Lund, H. *et al.* (2014) '4th Generation District Heating (4GDH). Integrating smart thermal grids into future sustainable energy systems.', *Energy*, 68, pp. 1–11. doi: 10.1016/j.energy.2014.02.089.

Majeed, J. H. and Aish, Q. (2021) 'A remote patient monitoring based on wban implementation with internet of thing and cloud server', *Bulletin of Electrical Engineering and Informatics*, 10(3), pp. 1640–1647. doi: 10.11591/eei.v10i3.1813.

Di Mascio, T. *et al.* (2019) 'Designing a personalizable ASD-oriented AAC tool: An action research experience', *Advances in Intelligent Systems and Computing*, 804(October 2018), pp. 200–209. doi: 10.1007/978-3-319-98872-6_24.

Mcarthur, J. J. (2015) 'A building information management (BIM) framework and supporting case study for existing building operations, maintenance and sustainability', *Procedia engineering*, 118, pp. 1104–1111. doi: 10.1016/j.proeng.2015.08.450.

Metke, A. R. and Ekl, R. L. (2010) 'Security Technology for Smart Grid Networks', 1(1), pp. 99–107.

Miorandi, D. *et al.* (2012) 'Ad Hoc Networks Internet of things : Vision , applications and research challenges', *Ad Hoc Networks*, 10(7), pp. 1497–1516. doi: 10.1016/j.adhoc.2012.02.016.

Miura, Y. *et al.* (2021) 'The Effectiveness of an Online Principal Preparation Program', *Research Institute for Progression of Knowledge*, 7(1), pp. 1–12.

Mohammed, Z. K. A. and Ahmed, E. S. A. (2017) 'World Scientific News WSN.', *World Scientific News*, 67(2), pp. 126–148. Available at: http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.psjd-b638cb4d-d68f-4f4c-afa5 ad309a7c4838%0Ahttps://www.infona.pl/resource/bwmeta1.element.psjd-8c8e8b68-9180-4879-85d8-a7870d5644e9.

Moukhliss, G., Filali Hilali, R. and Belhadaoui, H. (2019) 'A smart card digital identity check model for university services access', *ACM International Conference Proceeding Series*, Part F1481, pp. 3–6. doi: 10.1145/3320326.3320401.

Murdock, J. and Carroll, E. R. (2021) 'Simplifying and Visualizing the Ontology of Systems Engineering Models', *Sandia National Lab. (SNL-NM), Albuquerque, NM (United States)*. URL: 1814061 (osti.gov).

Naticchia, B., Corneli, A. and Carbonari, A. (2020) 'Framework based on building information modeling, mixed reality, and a cloud platform to support information flow in facility management', *Frontiers of Engineering Management*, 7(1), pp. 131–141. doi: 10.1007/s42524-019-0071-y.

Nedeva, V. and Dineva, S. (2015) 'Intelligent e-Learning with New Web Technologies', *The 10th International Conference on Virtual Learning ICVL*, 7(1), pp. 68–74.

Negri, E., Fumagalli, L. and Macchi, M. (2017) 'A review of the roles of Digital Twin in CPS-based production systems', *Procedia Manufacturing* ,11(June), pp. 939–948. doi: 10.1016/j.promfg.2017.07.198.

Neto, J., Jorge, A. and Nascimento, D. (2021) 'An Ontology for Fire Building Evacuation' *Proceedings of Sixth International Congress on Information and Communication Technology,* pp. 975-985.

OMG (2017) 'OMG Unified Modeling Language, Version 2.5.1', *OMG Unified Modeling Language Publication*, 91(5), p. 639. Available at: http://jultika.oulu.fi/files/isbn9789526214085.pdf%0Ahttp://www.ijarcsms.com/docs/paper/volume3/issue10/V3I10-0018.pdf%0Ahttps://www.omg.org/spec/UML/20161101/PrimitiveTypes.xmi.

Oriwoh, E. and Conrad, M. (2015) '"Things" in the Internet of Things: Towards a Definition', *International Journal of Internet of Things*, 4(1), pp. 1–5.

Pal, S. *et al.* (2020) 'Enrichment of semantic sensor network ontology: Description logics based approach', *Proceedings of the IEEE International Conference on Industrial Technology*, 2020–Febru, pp. 995–1000. doi: 10.1109/ICIT45562.2020.9067133.

Panas, A. and Pantouvakis, J. . (2010) 'Evaluating Research Methodology in Construction Productivity Studies', *The Built & Human Environment Review*, 3(1), pp. 63–85. Available at: www.tbher.org/index.php/tbher/article/download/34/36.

Pandey, G. (2012) 'The Semantic Web: An Introduction and Issues', *International Journal of Engineering Research and Applications*, 2(1), pp. 780–786. Available at: https://www.semanticscholar.org/paper/The-Semantic-Web-%3A-An-Introduction-and-Issues-Pandey/9289ad5d71376b4394aad026f84d2d3aacd145e4.

Papa, A. *et al.* (2020) 'E-health and wellbeing monitoring using smart healthcare devices: An empirical investigation', *Technological Forecasting and Social Change*, p. 119226. doi:10.1016/j.techfore.2018.02.018.

Parashar, M. *et al.* (2013) '2013 sixth International Conference on Contemporary Computing (IC3-2013) : 8-10 August 2013, Jaypee Institute of Information Technology, Noida, India', pp. 404–409.

Parno, B. *et al.* (2006) 'Secure Sensor Network Routing: A Clean-Slate Approach', *Proceedings of the 2006 ACM CoNEXT conference,* pp. 1-13.

Pauwels, P. *et al.* (2017) 'Enhancing the ifcOWL ontology with an alternative representation for geometric data', *Automation in Construction*, 80(April), pp. 77–94. doi: 10.1016/j.autcon.2017.03.001.

Pauwels, P. and Roxin, A. (2016) 'SimpleBIM: From full ifcOWL graphs to simplified building graphs', *eWork and eBusiness in Architecture, Engineering and Construction - Proceedings of the 11th European Conference on Product and Process Modelling, ECPPM 2016*, pp. 11–18.

Pauwels, P., Zhang, S. and Lee, Y. C. (2017) 'Semantic web technologies in AEC industry: A literature overview', *Automation in Construction*, 73, pp. 145–165. doi: 10.1016/j.autcon.2016.10.003.

Peng, G. C. and Annansingh, F. (2015) 'Experiences in applying mixed-methods approach in information systems research', *Research Methods: Concepts, Methodologies, Tools, and Applications*, 2–4, pp. 910–936. doi: 10.4018/978-1-4666-7456-1.ch041.

Perrig, A. *et al.* (2002) 'SPINS: Security Protocols for Sensor Networks', *Wireless networks*, pp. 521–534.

Perrig, A., Stankovic, J. and Wagner, D. (2004) 'Security in wireless sensor networks', *Communications of the ACM*, *47*(6), pp. 53–57.

Petrova-Antonova, D. and Ilieva, S. (2021) 'Digital twin modeling of smart cities', *Advances in Intelligent Systems and Computing*, 1253 AISC(September 2020), pp. 384–390. doi: 10.1007/978-3-030-55307-4_58.

Pivoto, D. G. S. *et al.* (2021) 'Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review', *Journal of Manufacturing Systems*, 58(December), pp. 176–192. doi: 10.1016/j.jmsy.2020.11.017.

Ponelis, S. R. (2015) 'Using interpretive qualitative case studies for exploratory research in doctoral studies: A case of information systems research in small and medium enterprises', *International Journal of Doctoral Studies*, 10, pp. 535–550. doi: 10.28945/2339.

Prabhakaran, A. *et al.* (2021) 'An investigation into macro BIM maturity and its impacts: a comparison of Qatar and the United Kingdom', *Architectural Engineering and Design Management*, 0(0), pp. 1–20. doi: 10.1080/17452007.2021.1923454.

Radha, V. and Reddy, D. H. (2012) 'A Survey on Single Sign-On Techniques', *Procedia Technology*, pp. 134–139. doi: 10.1016/j.protcy.2012.05.019.

Rahim, S. A., Mohd Nawi, M. N. and Nifa, F. A. A. (2016) 'Integrated project delivery (IPD): A collaborative approach to improve the construction industry', *Advanced Science Letters*, 22(5–6), pp. 1331–1335. doi: 10.1166/asl.2016.6764.

Rajput, Q. and Haider, S. (2011) 'Procedia Computer A comparison of ontology-based and reference-set-based semantic annotation frameworks', *Procedia Computer Science*, 3, pp. 1535–1540. doi: 10.1016/j.procs.2011.01.045.

Ramamoorthi, L. S. and Sarkar, D. (2020) 'Single Sign-On: A Solution Approach to Address Inefficiencies During Sign-Out Process', *IEEE Access*, 8, pp. 195675–195691. doi: 10.1109/access.2020.3033570.

Rashid, Y. *et al.* (2019) 'Case Study Method: A Step-by-Step Guide for Business Researchers', *International Journal of Qualitative Methods*, 18, pp. 1–13. doi: 10.1177/1609406919862424.

Rawat, D. B. and Bajracharya, C. (2015) 'Cyber security for smart grid systems: Status, challenges and perspectives', *Conference Proceedings - IEEE SOUTHEASTCON*, 2015–June(June). doi: 10.1109/SECON.2015.7132891.

Redmond, A. *et al.* (2012) 'Exploring how information exchanges can be enhanced through Cloud BIM', *Automation in Construction*, 24, pp. 175–183. doi: 10.1016/j.autcon.2012.02.003.

Rehman, A. U. *et al.* (2020) 'A trustworthy siot aware mechanism as an enabler for citizen services in smart cities', *Electronics (Switzerland)*, 9(6), pp. 1–19. doi: 10.3390/electronics9060918.

Rezgui, Y., Beach, T. and Rana, O. (2013) 'A governance approach for BIM management across lifecycle and supply chains using mixed-modes of information delivery', *Journal of Civil Engineering and Management*, 19(2), pp. 239–258. doi: 10.3846/13923730.2012.760480.

Ri, H. *et al.* (2021) 'A Review of Cyber Securities in Smart Grid Technology', *2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM)*, pp. 151–156.

Richard Fellows, A. and Liu (2015) 'for CONSTRUCTION', *des internationalen und auslåndischen Baurechts*, p. 807. Available at: http://link.springer.com/content/pdf/10.1007/b139091.pdf#page=853.

Roberto, J. and Davis, B. (2020) 'Towards the Ontologization of the Outsider Art Domain: Position Paper', *16th Joint ACL - ISO Workshop on Interoperable Semantic Annotation PROCEEDINGS*, (May), pp. 94–101. Available at: https://www.aclweb.org/anthology/2020.isa-1.11.

Roberts, C. J. *et al.* (2018) 'Digitalising asset management: concomitant benefits and persistent challenges', *International Journal of Building Pathology and Adaptation*, 36(2), pp. 152–173. doi: 10.1108/IJBPA-09-2017-0036.

Romigh, A. *et al.* (2017) '4D Scheduling: A Visualization Tool for Construction Field Operations', *53rd ASC Annual International Conference Proceeding*, pp. 395–404.

Rosen, R. *et al.* (2015) 'About the importance of autonomy and digital twins for the future of manufacturing', *Ifac-papersonline*, *48*(3), pp. 567–572.

Rosique, F., Losilla, F. and Pastor, J. Á. (2017) 'A Domain Specific Language for Smart Cities', *the proceedings of the 4th international electronic conference on sensors and applications*, 2(3), p. 148. doi: 10.3390/ecsa-4-04926.

Rupani, A. (2016) 'A Review of Technology Paradigm for IOT on FPGA A Review of Technology Paradigm for IOT on FPGA', *IJARCCE-International Journal of Advanced Research in Computer and Communication Engineering*, pp. 61–64.

El Saddik, A. (2018) 'Digital Twins: The Convergence of Multimedia Technologies', *IEEE Multimedia*, 25(2), pp. 87–92. doi: 10.1109/MMUL.2018.023121167.

Sadeghioon, A. M. *et al.* (2014) 'SmartPipes: Smart wireless sensor networks for leak detection in water pipelines', *Journal of Sensor and Actuator Networks*, 3(1), pp. 64–78. doi: 10.3390/jsan3010064.

Saravana Kumar, C. S. and Santhosh, R. (2020) 'Effective information retrieval and feature minimization technique for semantic web data', *Computers and Electrical Engineering*, 81, p. 106518. doi: 10.1016/j.compeleceng.2019.106518.

Sari, Y. C., Wahyuningrum, C. A. and Kresnanto, N. C. (2020) 'Building Information Modeling (BIM) for Dams-Literature Review and Future Needs', *Journal of the Civil Engineering Forum*, 6(1), p. 61. doi: 10.22146/jcef.51519.

Satamraju, K. P. and Malarkodi, B. (2020) 'Proof of concept of scalable integration of internet of things and blockchain in healthcare', *Sensors (Switzerland)*, 20(5). doi: 10.3390/s20051389.

Saunders et al. (2009) 'Research Methods for Business Students', *Pearson*, p. 649.

Saunders, M., Lewis, P. and Thornhill, A. (2019) 'Understanding research philosophy and approaches to theory development', *Research Methods for Business Students*, ISBN: 978-1-292-20878-7.

Schlagwort, A. (2011) 'What's new in description logics', *Informatik-Spektrum*, *34*(5), pp.434–442.

Sebastian, R. (2011) 'Changing roles of the clients, architects and contractors through BIM', *Engineering, Construction and Architectural Management*, 18(2), pp. 176–187. doi: 10.1108/09699981111111148.

Seeger, J., Deshmukh, R. A. and Broring, A. (2018) 'Running distributed and dynamic IoT choreographies', *2018 Global Internet of Things Summit, GIoTS 2018*, pp. 1–6. doi: 10.1109/GIOTS.2018.8534570.

Shin, D. (2009) 'Ubiquitous city: Urban technologies, urban infrastructure and urban informatics', *Journal of Information Science*, 35(5), pp. 515–526. doi: 10.1177/0165551509100832.

Shoewu, O. *et al.* (2012) 'Pjst13_1_300', *Pacific Journal of Science and Technology*, 13(1), pp. 300–307.

Siksha 'O' Anusandhan, Bhubaneswar, O. (2020) 'Attendance Management System Using RFID', *International Journal of Advanced Research in Engineering and Technology (IJARET),* pp. 2013–2015. doi: 10.34218/IJARET.11.12.2020.029.

Simperl, E. (2009) 'Reusing ontologies on the Semantic Web: A feasibility study', *Data and Knowledge Engineering*, 68(10), pp. 905–925. doi: 10.1016/j.datak.2009.02.002.

Snaith, B., Hardy, M. and Walker, A. (2011) 'Emergency ultrasound in the prehospital setting: The impact of environment on examination outcomes', *Emergency Medicine Journal*, 28(12), pp. 1063–1065. doi: 10.1136/emj.2010.096966.

Söbke, H. *et al.* (2021) 'An IFC schema extension for BIM-based description of wastewater treatment plants', *Automation in Construction*, 129(July). doi: 10.1016/j.autcon.2021.103777.

Sorek-Hamer, M., Just, A. C. and Kloog, I. (2016) 'Satellite remote sensing in epidemiological studies', *Current Opinion in Pediatrics*, 28(2), pp. 228–234. doi: 10.1097/MOP.0000000000000326.

Sridhar, S., Hahn, A. and Govindarasu, M. (2012) 'Cyber – Physical System Security for the Electric Power Grid', *Proceedings of the IEEE*, 100(1), pp. 210–224. doi: 10.1109/JPROC.2011.2165269.

'State of the Nation Survey' (2021), *UK BIM alliance*, URL: UKBIMA-State-of-the-Nation-Survey-Report-2021.pdf (ukbimalliance.org).

Steinleitner, J. (2020) 'Verteilte Policy-basierte Autorisierung mit OAuth 2.0 und OpenID Connect', *Doctoral dissertation, Hochschule für Angewandte Wissenschaften Landshut* URL:Steinleitner, J. (2020) 'Verteilte Policy-basierte... - Google Scholar>> In google scholar "right style?"

Steinmetz, C. and Rettberg, A. (2018) 'Internet of Things Ontology for Digital Twin in Cyber Physical Systems', *2018 VIII Brazilian symposium on computing systems engineering (SBESC),* pp. 154–159. doi: 10.1109/SBESC.2018.00030.

Stiles, J. (2003) 'A philosophical justification for a realist approach to strategic alliance research', *Qualitative Market Research: An International Journal*, 6(4), pp. 263–271. doi: 10.1108/13522750310495346.

Stojkovski, V. and Nenovski, B. (2020) 'the Usage of Decision Support Systems in North Macedonian Companies', *Horizons International Journal*, 25, pp. 113–129. doi: 10.20544/HORIZONS.A.25.2.20.P07.

Sturdee, M. *et al.* (2021) 'A Visual Exploration of Cybersecurity Concepts', *ACM International Conference Proceeding Series*. doi: 10.1145/3450741.3465252.

Suárez-Figueroa, M. C., Gómez-Pérez, A. and Fernández-López, M. (2015) 'The NeOn Methodology framework: Ascenario-based methodology for ontology development', *Applied Ontology*, 10(2), pp. 107–145. doi: 10.3233/AO-150145.

Sugiharto, W. *et al.* (2019) 'Multiple Smart Home Controlling System using Database Replication Method', *1st International Conference on Computer Science and Engineering Technology*, pp. 2–8. doi: 10.4108/eai.24-10-2018.2280553.

Sun, S., Lannom, L. and Boesch, B., (2003) 'Handle system overview', *Network Working Group Request for Comments: 3650 Category: Informational*, pp. 1–21.

Taddeo, M., McCutcheon, T. and Floridi, L. (2019) 'Trusting artificial intelligence in cybersecurity is a double-edged sword', *Nature Machine Intelligence*, 1(12), pp. 557–560. doi: 10.1038/s42256-019-0109-1.

Tahmid, T. and Hossain, E. (2018) 'Density based smart traffic control system using canny edge detection algorithm for congregating traffic information', *3rd International Conference on Electrical Information and Communication Technology, EICT 2017*, 2018–Janua(December), pp. 1–5. doi: 10.1109/EICT.2017.8275131.

Tang, S. *et al.* (2019) 'Automation in Construction A review of building information modeling (BIM) and the internet of things (IoT) devices integration : Present status and future trends', *Automation in Construction*, 101(January), pp. 127–139. doi: 10.1016/j.autcon.2019.01.020.

Tang, X. *et al.* (2019) 'Ultra-Wideband Patch Antenna for Sub-6 GHz 5G Communications', *2019 IEEE International Workshop on Electromagnetics: Applications and Student Innovation Competition, iWEM 2019 - Proceedings*, pp. 2019–2021. doi: 10.1109/iWEM.2019.8887933.

Tao, F. *et al.* (2014) 'IoT-Based Intelligent Perception and Access of Manufacturing Resource Toward Cloud', *IEEE transactions on industrial informatics*, 10(2), pp. 1547–1557. doi: 10.1109/TII.2014.2306397.

Tao, F. *et al.* (2019) 'Digital Twin in Industry: State-of-the-Art', *IEEE Transactions on Industrial Informatics*, 15(4), pp. 2405–2415. doi: 10.1109/TII.2018.2873186.

Tao, F. E. I. and Zhang, M. (2017) 'Digital Twin Shop-Floor: A New Shop-Floor Paradigm Towards Smart Manufacturing', *IEEE Access*, pp.20418-20427.

Tao, F. and Qi, Q. (2019) 'New IT Driven Service-Oriented Smart Manufacturing : Framework and Characteristics', *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 49(1), pp. 81–91. doi: 10.1109/TSMC.2017.2723764.

Tapia-Leon, M. *et al.* (2019) 'Extension of the BIdo ontology to represent scientific production', *ACM International Conference Proceeding Series*, Part F1481(March), pp. 166–172. doi: 10.1145/3318396.3318422.

Tarasov, V., Seigerroth, U. and Sandkuhl, K. (2019) 'Ontology development strategies in industrial contexts', *Lecture Notes in Business Information Processing*, 339(July 2018), pp. 156–167. doi: 10.1007/978-3-030-04849-5_14.

Taylor, K. *et al.* (2019) 'The semantic sensor network ontology, revamped', *CEUR Workshop Proceedings*, 2576, pp. 1–9.

Technology, N. I. of S. and (2017) 'FIPS PUB 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors', *Nist-Fips,* pp. 1-87.

Tellez, M., El-Tawab, S. and Heydari, H. M. (2016) 'Improving the security of wireless sensor networks in an IoT environmental monitoring system', *2016 IEEE Systems and Information Engineering Design Symposium, SIEDS 2016*, pp. 72–77. doi: 10.1109/SIEDS.2016.7489330.

Thakker, D. *et al.* (2020) 'SAREF4INMA: A SAREF extension for the industry and manufacturing

domain', *Semantic Web*, 11(6), pp. 911–926. doi: 10.3233/SW-200402.

Tran, L.A. *et al.* (2021) 'Enhancement of Robustness in Object Detection Module for Advanced Driver Assistance Systems'; *2021 International Conference on System Science and Engineering (ICSSE),* pp. 158-163. IEEE.

Tuegel, E. J. *et al.* (2011) 'Reengineering Aircraft Structural Life Prediction Using a Digital Twin', *International Journal of Aerospace Engineering*, doi: 10.1155/2011/154798.

Turk, R. J. (2005) 'Cyber Incidents Involving Control Systems' *Idaho National Laboratory (INL)*, doi: 10.2172/911775.

Upadhyay, D. and Sampalli, S. (2020) 'SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations', *Computers and Security*, 89(January), p. 101666. doi: 10.1016/j.cose.2019.101666.

Vajpayee, A. and Ramachandran, K. K. (2019) 'Reconnoitring artificial intelligence in knowledge management', *International Journal of Innovative Technology and Exploring Engineering*, 8(7), pp. 114–117.

Venugopal, M. and Eastman, C. (2010) 'Engineering Semantics of Model Views for Building', *CIB W78 2010: 27th International Conference –Cairo*, pp. 16–18.

Vinet, L. and Zhedanov, A. (2011) 'A "missing" family of classical orthogonal polynomials', *Journal of Physics A: Mathematical and Theoretical*, 44(8). doi: 10.1088/1751-8113/44/8/085201.

Voightmann (2004) 'Generating quality software *specifications* for decision support: a novel approach,' *Massachusetts Institute of Technology*.

Wang, Z., Sun, J. and Hutchison, D. (2016) 'Semantic Technology' *6th Joint International Conference, JIST 2016, Singapore, Singapore, November 2-4, 2016, Revised Selected Papers* (Vol. 10055). Springer.

Weaver, K. and Olson, J. K. (2006) 'Understanding paradigms used for nursing research', *Journal of Advanced Nursing*, 53(4), pp. 459–469. doi: 10.1111/j.1365-2648.2006.03740.x.

Weber, R. H. (2010) 'Internet of Things - New security and privacy challenges', *Computer Law and Security Review*, 26(1), pp. 23–30. doi: 10.1016/j.clsr.2009.11.008.

Wu, Z. *et al.* (2019) 'BIM-based visualization research in the construction industry: A network analysis', *International Journal of Environmental Research and Public Health*, 16(18). doi: 10.3390/ijerph16183473.

Yamamoto, S., Matsumoto, S. and Nakamura, M. (2012) 'Using cloud technologies for large-scale house data in smart city', *CloudCom 2012 - Proceedings: 2012 4th IEEE International Conference on Cloud Computing Technology and Science*, pp. 141–148. doi: 10.1109/CloudCom.2012.6427546.

Zainal, Z. (2007) 'The Case Study as a Research Method', *Jurnal Kemanusiaan bil*, pp. 15–15. doi: 10.4135/9781473915480.n2.

Zhang, H. and Zhu, L. (2011) 'Internet of Things: Key technology, architecture and challenging problems', *Proceedings - 2011 IEEE International Conference on Computer Science and Automation Engineering, CSAE 2011*, 4, pp. 507–512. doi: 10.1109/CSAE.2011.5952899.

Zhang, Y. *et al.* (2016) 'SenStore: A Scalable Cyberinfrastructure Platform for Implementation of Data-to-Decision Frameworks for Infrastructure Health Management', *Journal of Computing in Civil Engineering*, 30(5), p. 04016012. doi: 10.1061/(asce)cp.1943-5487.0000560.

Zhao, D. *et al.* (2015) 'Building Collaborative Construction Skills through BIM-integrated Learning Environment', *International Journal of Construction Education and Research*, 11(2), pp. 97–120. doi: 10.1080/15578771.2014.986251.

Zhao, W., Beach, T. H. and Rezgui, Y. (2018) 'A systematic mixed-integer differential evolution approach for water network operational optimization', *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 474(2217). doi: 10.1098/rspa.2017.0879.

Appendix A: industry survey and chart of experts' responses

Access Management for Digital Twins in the Built Environment

Page 1

Overview:

Cardiff University is currently studying the subject of Cybersecurity for Digital Twins in the built environment

This work is focusing on how security concepts can be applied to digital twins to provide new possibilities for cyber physical systems (CPSs) to enhance the use of IOT in conjunction with information models (such as BIM) in the built environment.

We invite you to participate in this questionnaire with a view of determining the barriers to the use of cyber physical systems, cyber physical systems current practices, usage of digital twins in your organization and the requirements for enhancing Cybersecurity for Digital Twins in the built environment.

All data collected in this survey will be held securely in accordance with the data protection act and GDPR regulations. Personal data collected (your e-mail address) will only be used to contact you in follow up to this survey, and this will only happen if you allow it. Cookies and personal data stored by your Web browser, are not used in this survey.

Page 2

1- Please specify your length of experience working in the built environment. *Required*

- 0-10 years
- 10-20 years
- 20-30 years
- More than 30 years

2- Please specify your current role in your organisation. *Required*

- Structural engineer
- Architecture engineer
- BIM manager
- Developer
- Other

3- Please specify the type of your organisation. *Required*

- Structural design
- Strategic Planning
- Multidisciplinary engineering consultancy
- AEC multidisciplinary (design & construction)
- Other

4- Does your organisation use any form of Cyber-Physical/IOT Systems as part of their work in the built environment? *Required*

- ○ Yes, please answer the following question
- ○ No, skip the next question

5- What are the problems have you faced during using Cyber-Physical/IOT Systems? *Optional*

- ☐ Data protection and data security
- ☐ Data exchanging
- ☐ Lack of benefit quantification
- ☐ Other

6- Is your organisation considering the use of cyber physical systems? *Required*

- ○ Yes, in the short term
- ○ Yes, in the long term
- ○ No
- ○ Other

7- Does your organisation make use of Digital Twins in their work in built environment? *Required*

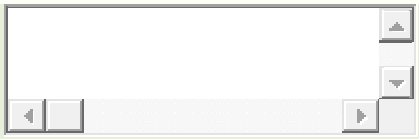
- ○ Yes
- ○ No

8- Have you deployed digital twins in any major project in the built environment domain? *Required*

- Yes, please answer the following questions
- No, skip to Q21

9- Can you describe briefly the type of project this was? *Optional*

10- What advantages did you find of using a Digital Twins during the project? *Optional*



11- What barriers did you find to using a Digital Twin? *Optional*

- Training skills
- Limited access to data
- Cost
- Applicable technology
- Other

12- Do you utilise a dedicated cybersecurity team for management and design of digital twins/cyber physical systems? *Optional*

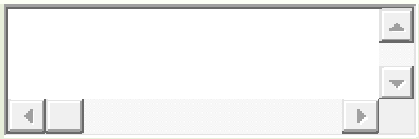
- Yes

- [ ] No

13- What issues do you have managing threats in digital twins/cyber physical system? *Optional*

- [ ] Lack of export in security management
- [ ] Lack of technology
- [ ] Cost
- [ ] Other

14- How is access to data in your digital twins/cyber physical systems managed? *Optional*



15- What type of authentication you are using? *Optional*

- [ ] Log in (username and password)
- [ ] Biometric (iris scans, fingerprint scans and voice recognition)
- [ ] Other

16- Are there controls to classify data in terms of criticality and sensitivity? *Optional*

- [ ] Yes
- [ ] No

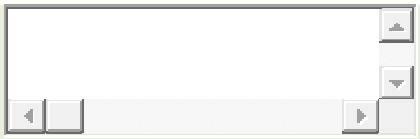
17- What type of controls to classify data you are using? *Optional*

- [ ] Availability
- [ ] Confidentiality
- [ ] Integrity

18- Are there tools and processes to find out and prevent sensitive data from leaving the digital twins/cyber physical systems? *Optional*

- ( ) Yes
- ( ) No

19- What type of tools you are using? *Optional*



20- Do you have the ability to monitor digital twins/cyber physical systems to detect anomalous activities? *Optional*

- ( ) Yes
- ( ) No

21- Do you plan to make use of digital twins/cyber physical systems in your organization in the future? *Required*

- ( ) Yes
- ( ) No

22- In what context does your organisation use/plan to use digital twin technology? *Required*

- ☐ Urban design development
- ☐ Data analysis
- ☐ Building operation
- ☐ Control access
- ☐ Other

This part of the survey uses a table of questions, view as separate questions instead?

23- Which criteria are important to you regarding to enhance adoption of Digital Twins /Cyber Physical Systems in the built environment? *Required*

Please don't select more than 1 answer(s) per row.

Please select between 1 and 5 answers.

Please don't select more than 5 answer(s) in any single column.

	(Extremely important)	(Very important)	(Somewhat important)	(Not at all important)
Training skills	☐	☐	☐	☐
Relevant technology	☐	☐	☐	☐
Developing a smart application architecture	☐	☐	☐	☐
smart grid	☐	☐	☐	☐

Expand BIM specifications to become IoT compliant	☐	☐	☐	☐

This part of the survey uses a table of questions, view as separate questions instead?

24- Which criteria are important to you regarding to enhance adoption of Cybersecurity for Digital Twins /Cyber Physical Systems in the built environment? *Required*

Please don't select more than 1 answer(s) per row.

Please select between 1 and 5 answers.

Please don't select more than 5 answer(s) in any single column.

	(Extremely important)	(Very important)	(Somewhat important)	(Not at all important)
Training skills	☐	☐	☐	☐
Relevant technology	☐	☐	☐	☐
Developing a smart application architecture	☐	☐	☐	☐
smart grid security	☐	☐	☐	☐
Expand BIM specifications to become IoT compliant	☐	☐	☐	☐

1- Please specify your length of experience working in the built environment.

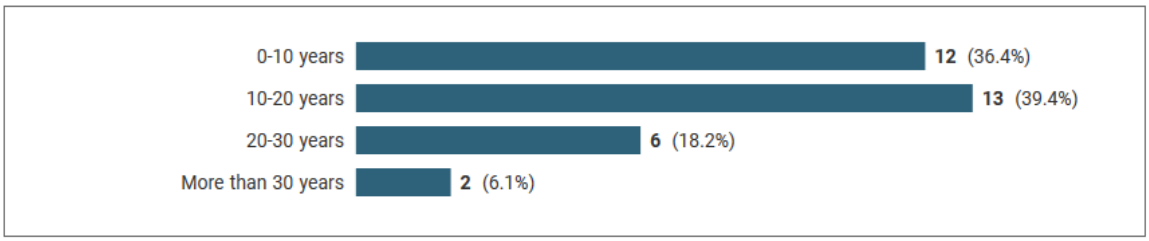


Fig. 1: Work Experience

2- Please specify your current role in your organisation.

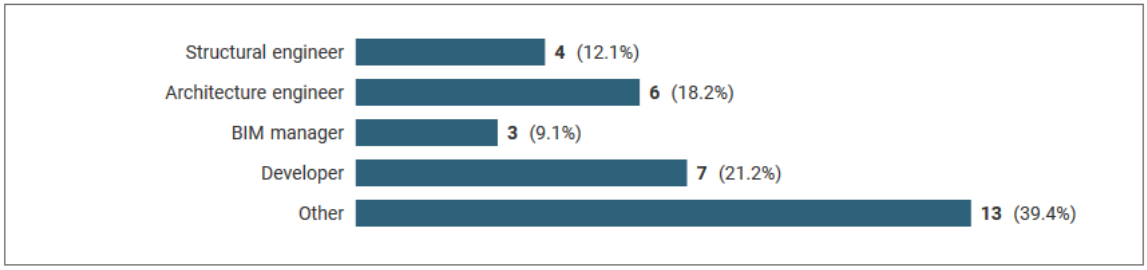


Fig 2: current roles

Question 2.a: If you selected Other, please specify:

Showing all 13 responses Show less	
Director	576481-576472-57192131
Electric engineering	576481-576472-57199505
Research and development engineer	576481-576472-57315381
Urban planner	576481-576472-57322596
Founder urban design firm	576481-576472-57364629
R&D Project manager	576481-576472-57419750
PostDoctoral Researcher	576481-576472-57420612
Innovation manager	576481-576472-57420211
Researcher	576481-576472-57430108
Professor: Education & Research	576481-576472-57450940
University of Technology	576481-576472-57470096
R&D	576481-576472-57839240
head of department	576481-576472-57880518

Fig 3. Verify roles

3- Please specify the type of your organisation.

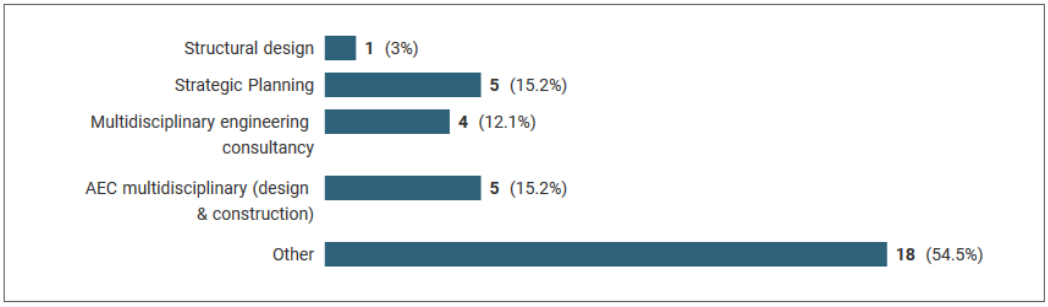


Fig 4: Organisations Types

Question 3.a: If you selected Other, please specify:

Showing all 18 responses Show less	
real eastat	576481-576472-57113062
ICT	576481-576472-57192131
Extraction company	576481-576472-57199257
Extracting company	576481-576472-57199472
Extracting company	576481-576472-57199505
IT company	576481-576472-57315381
Urban design	576481-576472-57364629
University	576481-576472-57420612
Research institute	576481-576472-57420211
Research institution	576481-576472-57430108
Rto	576481-576472-57431153
University	576481-576472-57450940
Research and Development center.	576481-576472-57463005
Research and Teaching	576481-576472-57470096
Public client	576481-576472-57477917
IT	576481-576472-57516456
Research Center	576481-576472-57839240
research	576481-576472-57880518

Fig 5: Various types of the organizations

4- Does your organisation use any form of Cyber-Physical/IOT Systems as part of their work in the built environment?

Fig 6: Use Cyber-Physical/IOT Systems

5- What are the problems have you faced during using Cyber-Physical/IOT Systems?

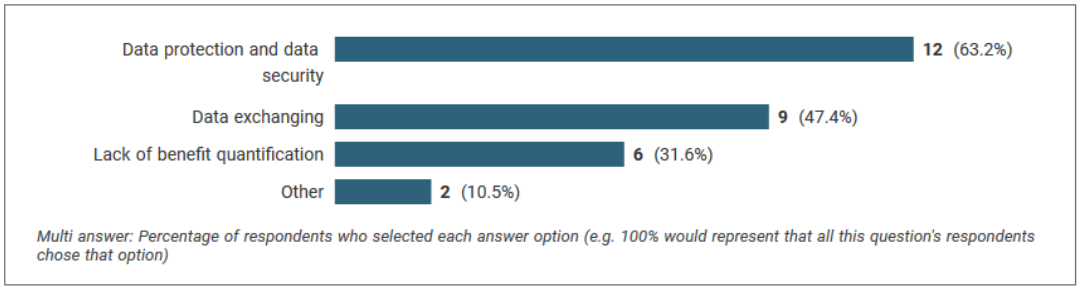


Fig 7: Problems in Cyber-Physical/IOT Systems

Question 5.a: If you selected Other, please specify:

Showing all 2 responses	
Standardization - all commercial Open Platforms basically define their own APIs, protocols, and encodings. This causes big interoperability problems. Also handling access control over different platforms from different providers in a uniform way has not been handled well so far. This problem also extends to the handling of securing the access to distributed services and platforms.	576481-576472-57450940
- No standar data format	576481-576472-57463005

Fig 8: Other problems in Cyber-Physical/IOT Systems

6- Is your organisation considering the use of cyber physical systems?

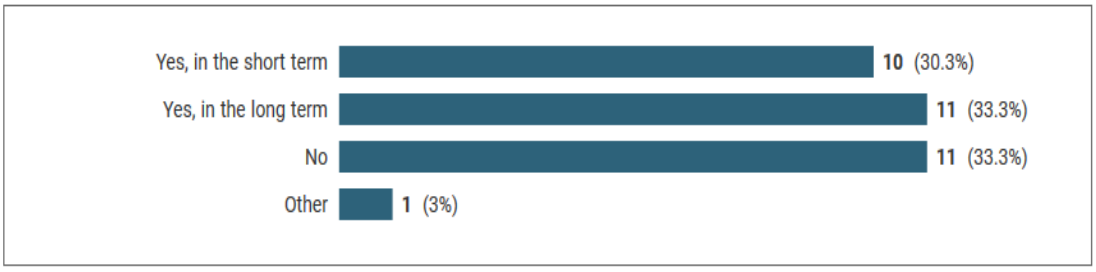


Fig 9: Considering the use of cyber physical systems

Question 6.a: If you selected Other, please specify:

Showing 1 response	
Our organization is on the early stages regarding these kinds of systems	576481-576472-57386592

Fig 10: Other considering the use of cyber physical systems

7- Does your organisation make use of Digital Twins in their work in built environment?

Fig 11: Using the Digital Twins in the organisations

8- Have you deployed digital twins in any major project in the built environment domain?

Fig 12: Depending Digital Twins

9- Can you describe briefly the type of project this was?

Showing all 13 responses Show less	
hr with finance	576481-576472-57113062
Multiple Smart cities	576481-576472-57192131
Design cities	576481-576472-57354586
PMO smart for project	576481-576472-57364234
digital twins (calibrated numerical models of the studied building) are commonly used in research and teaching to perform fault detection, optimization, renovation plan, long term estimation of energy usage, urban-scale modelling, optimum control of HVAC system (Model Predictive Control).	576481-576472-57420612
Digital Twins of bridges, Digital Twins of energy systems in buildings and cities	576481-576472-57420211
Creation of digital environments for the acquistion of data	576481-576472-57430108
We are creating a digital twin in two building that are monitoring building energy consumption, thermal performance, and indoor air quality	576481-576472-57438242
We have created and established semantic 3D city models for many different cities worldwide including Berlin, districts of London, New York City, Melbourne etc. Like BIM models, semantic 3D city models are also information models. In contrast to BIM models, they have a lower level of detail regarding the individual objects, but typically contain all the objects of the physical environment for different types including buildings, bridges, tunnels, infrastructure, vegetation, water bodies, and terrain. Every city object is considered the digital twin of the respective physical object. IoT devices are connected with the city models down to the level of linking sensor data streams with specific properties of urban objects.	576481-576472-57450940
- Optimize building Management. We integrated BIM and building process with Artificial Intelligent.	576481-576472-57463005
Digital twin is in major projects the result as it is dtermined in Finnish InfraBIM Requirements.	576481-576472-57477917
H2020, BIM enrichment with real data coming from BACN	576481-576472-57839240
lab model of a suspension bridge	576481-576472-57880518

Fig 13: Types projects use Digital Twins

10- What advantages did you find of using a Digital Twins during the project?

Showing all 11 responses Show less	
Digital twins will really help in transforming cites to smart cites and will support IoT specially in design phase. It is in our road map.	576481-576472-57192131
Facilitate the design	576481-576472-57354586
...	576481-576472-57364234
Realtime monitoring and performance analysis	576481-576472-57420211
Realiable representation of the physical system	576481-576472-57430108
A new visual way to read sensors easily and implementing tools for facility managment	576481-576472-57438242
Computation of key performance indicators for urban districts and entire cities can often be completely computed on the basis of the digital twin. In many cases, the required input data for the many different kinds of simulations (energy consumption and production, traffic flows, noise dispersion, air quality) can directly be derived from the digital twin. We can clone the digital twin and create scenarios by modifying the semantic 3D city model and can immediately run the same stack of computations and simulations on the modified digital twin for impact assessment of planned actions.	576481-576472-57450940
A best understanding by the building manager of the building process. A holistic action.	576481-576472-57463005
Better communication between different project parties, cost savings, better design solutions.	576481-576472-57477917
interoperability, visualization as a whole	576481-576472-57839240
real time assessment of structural behaviour, damages etc.	576481-576472-57880518

Fig 14: Advantages of using a Digital Twins during the project

11- What barriers did you find to using a Digital Twin?

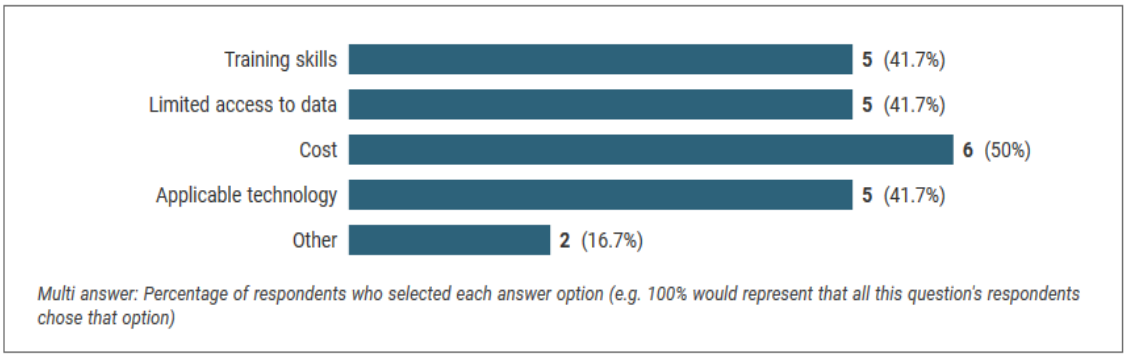


Fig 15: Barriers of using a Digital Twin

Question 11.a: If you selected Other, please specify:

Showing all 2 responses	
Keeping the digital twin for entire urban districts (or even cities) up-to-date is very difficult. Furthermore, unlike in many other industries the data that belong to digital urban twins is not in the hand of a single owner (like the manufacturer of a machine / device), but spread over many stakeholders. But if the data is in the hand of many stakeholders - who is responsible to maintain / assess data integrity?	576481-576472-57450940
Resistance to new things or this is how it has been done earlier	576481-576472-57477917

Fig 16: Other barriers of using a Digital Twin

12- Do you utilise a dedicated cybersecurity team for management and design of digital twins/cyber physical systems?

Fig 17: Cybersecurity team

13- What issues do you have managing threats in digital twins/cyber physical system?

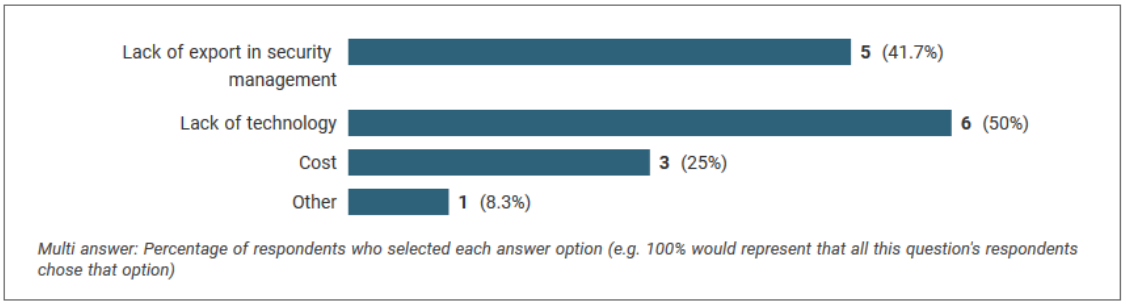


Fig 18: Issues managing threats in digital twins/cyber physical system

Question 13.a: If you selected Other, please specify:

Showing 1 response	
interoperability	576481-576472-57839240

Fig 19: Other issue managing threats in digital twins/cyber physical system

14- How is access to data in your digital twins/cyber physical systems managed?

Showing all 9 responses Show less	
physical system became very easy Digital twin still not implemented.	576481-576472-57192131
By a dedicated team	576481-576472-57354586
...	576481-576472-57364234
Usually run manually on local computer behind proxi. Security is not big problem, but it should be considered, especially when dealing with pilot project of occupied buildings	576481-576472-57420612
By the researchers and project leaders	576481-576472-57420211
It depends on the context and availability	576481-576472-57430108
We are using the full range of Open API specification standards issued by the Open Geospatial Consortium (OGC), i.e. Web Feature Service (WFS), Web Processing Service (WPS), 3D Portrayal Service (3DPS), Catalog Service for the Web (CS/W), Sensor Web Enablement (including SensorThings API), and employ and also provide implementations for these. The semantic 3D city models are represented and stored according to the CityGML standard. BIM models can be incorporated into the city models, but then are converted to CityGML before. For access control we have shown how to apply oauth2, SAML2, and OpenID connect to establish a security federation to facilitate single-sign-on over the distributed web services and stakeholders.	576481-576472-57450940
We use a open format; Node Red.	576481-576472-57463005
BACS network	576481-576472-57839240

Fig 20. Access to data in the digital twins/cyber physical systems.

15- What type of authentication you are using?

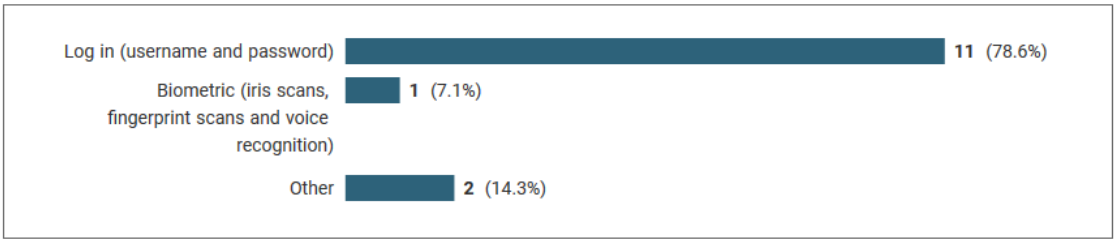


Fig 21. Types of authentications

Question 15.a: If you selected Other, please specify:

Showing all 2 responses	
two factor authentication	576481-576472-57192131
We are using technologies like Kerberos and Keycloak to allow different kinds of authentication for the respective services.	576481-576472-57450940

Fig 22. Other types of authentications

16- Are there controls to classify data in terms of criticality and sensitivity?

Fig 23. Classification data

17- What type of controls to classify data you are using?

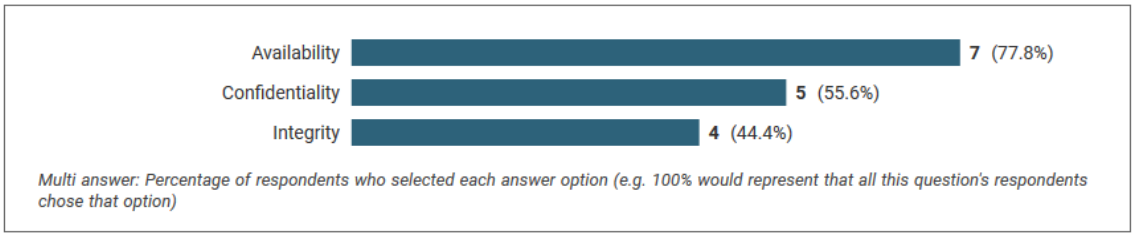


Fig 24. Type of controls to classify data

18- Are there tools and processes to find out and prevent sensitive data from leaving the digital twins/cyber physical systems?

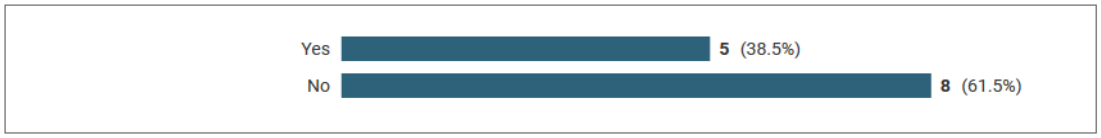


Fig 25. Tools to prevent sensitive data from leaving the digital twins/cyber physical systems

19- What type of tools you are using?

Showing all 4 responses	
Open source for IoT platform, gateway and physical sensors	576481-576472-57192131
Architectural programs	576481-576472-57354586
Local	576481-576472-57364234
Access control mechanisms by using implementations of oauth2, SAML2, OpenID Connect and their implementation on web services., e.g. in Apache Tomcat and Webservers.	576481-576472-57450940

Fig 26. Various tools to prevent sensitive data from leaving the digital twins/cyber physical systems

20- Do you have the ability to monitor digital twins/cyber physical systems to detect anomalous activities?

Fig 27. Ability to monitor digital twins/cyber physical systems to detect anomalous activities

21- Do you plan to make use of digital twins/cyber physical systems in your organization in the future?

Fig 28. Using the digital twins/cyber physical systems in the organizations in the future

Question 21.a: What are your plans in this area?

Showing all 18 responses Show less	
Involving all stakeholders in the urban deign process to get the most out of information communicate technology	576481-576472-57174176
digital twin	576481-576472-57192131
Integrate into IoT devices	576481-576472-57315381
Confidential	576481-576472-57386592
Collect and make use of data which can be used to improve performance or maintenance, or using actuators to take some actions.	576481-576472-57390910
under analysis	576481-576472-57419750
Many different project to implement and test IoT in buildings	576481-576472-57420612
Upscaling of Digital Twins in buildings and infrastructure	576481-576472-57420211
EU research and development project	576481-576472-57421652
Creation of digital twins/cyber physical systems for interoperability and prediction techniques about performance	576481-576472-57430108
We are more or less in the reseaech phase.	576481-576472-57431153
Implementing tools for facility managment	576481-576472-57438242
We are currently building up digital twins for all agricultural research stations including buildings, infrastructure, but also crop fields and laboratories for our university.	576481-576472-57450940
We want grow in the solution. And integrated new algorithms for optimization of building in all phases; construction, Management,...	576481-576472-57463005
To test in a research project	576481-576472-57470096
Power consumption, security, structure durability and failures	576481-576472-57497057
in research projetcs, demosites and our own builidings	576481-576472-57839240
demonstrators in real scale	576481-576472-57880518

Fig 29. Plans in different areas

22- In what context does your organisation use/plan to use digital twin technology?

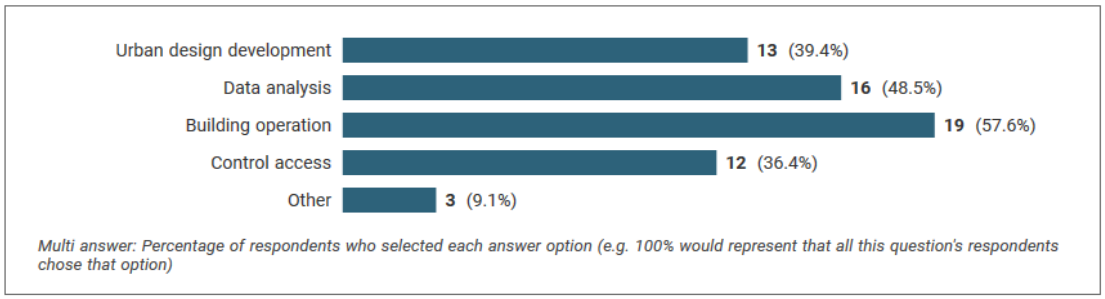


Fig 30. Using Digital Twins technology

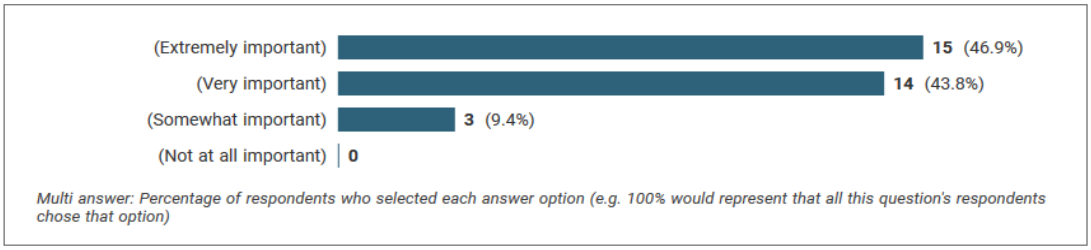
Question 22.a: If you selected Other, please specify:

Showing all 3 responses	
Usage of semantic 3D city models (city information modeling) on the level of city districts and entire cities to monitor KPIs from different application domains like energy, mobility, environment.	576481-576472-57450940
demolition reuse of materials	576481-576472-57463005
Additional third party services like energy efficiency services	576481-576472-57839240

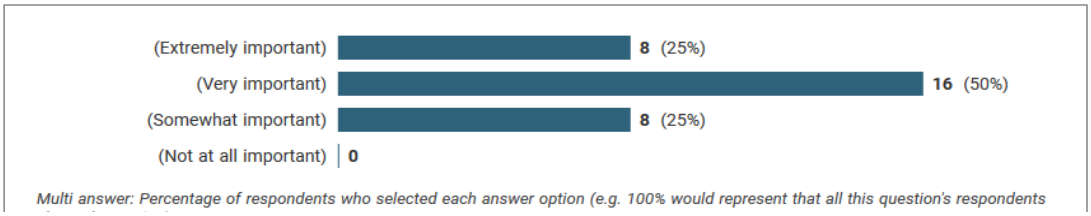
Fig 31. Other using Digital Twins technology

23- Which criteria are important to you regarding to enhance adoption of Digital Twins /Cyber Physical Systems in the built environment?

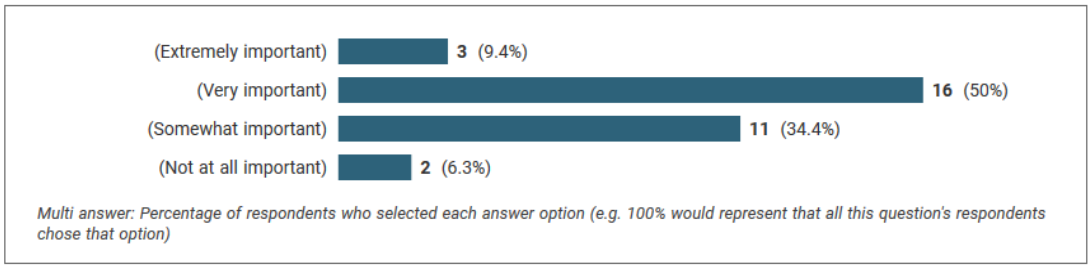
23.1 Training skills



23.2 Relevant technology



23.4 smart grid



23.5 Expand BIM specifications to become IoT compliant

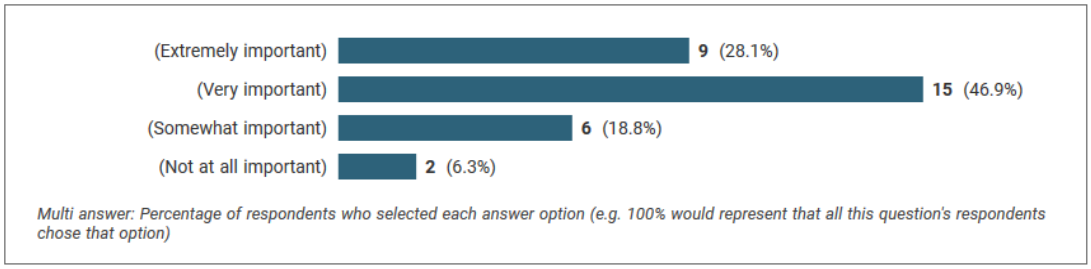


Fig 32. Important criteria enhance adoption of Digital Twins /Cyber Physical Systems

24- Which criteria are important to you regarding to enhance adoption of Cybersecurity for Digital Twins /Cyber Physical Systems in the built environment?

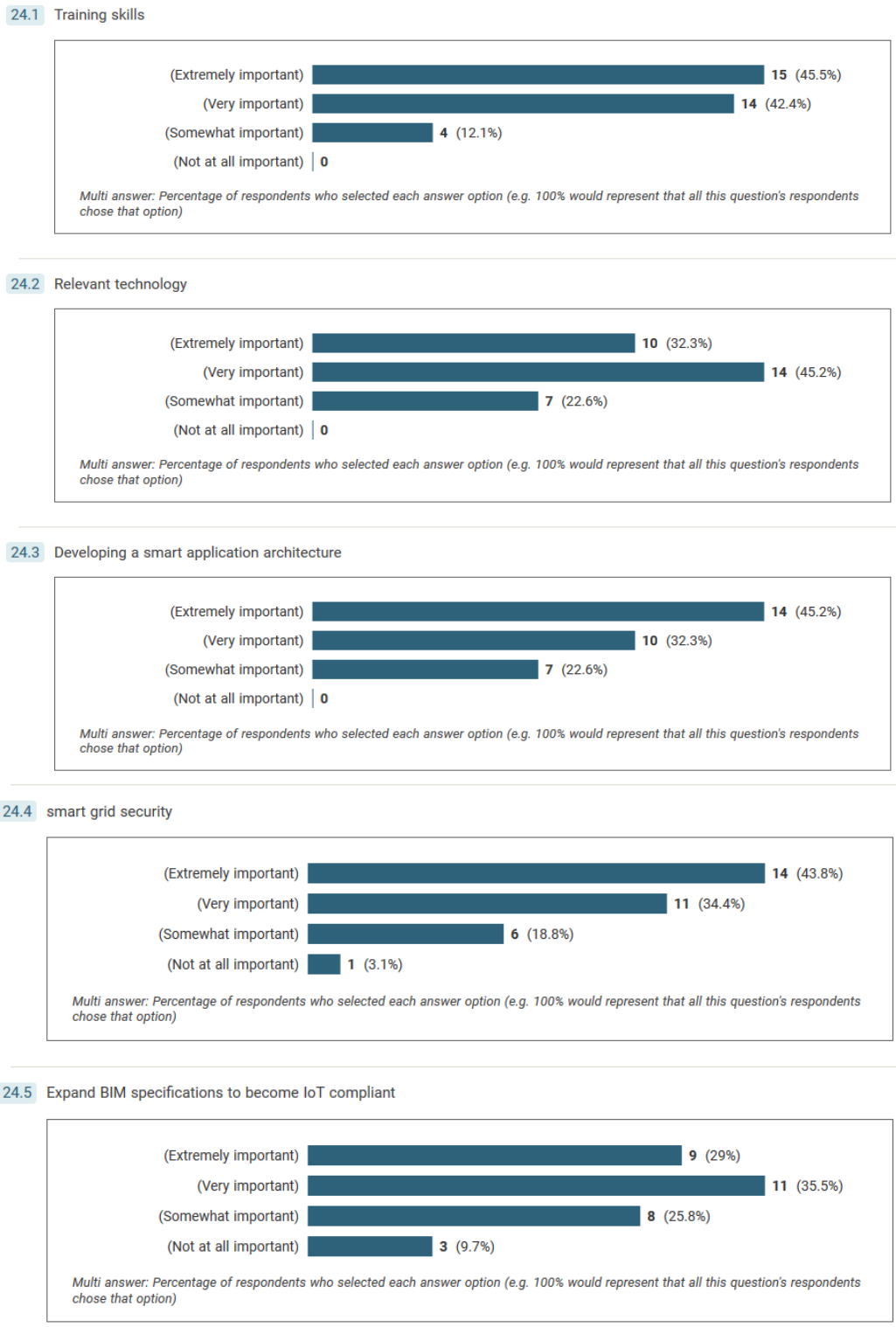


Fig 33. Important criteria enhance adoption of Cybersecurity for Digital Twins /Cyber Physical Systems

Appendix B: Built environment case studies

Table 1 Smart parking system access control

Data Description	Data Controller	Confidentiality Restriction	Integrity Restrictions	Availability Restrictions	Notes
• Parking System General Information • Operator Contact information	System Administrator	Available to everyone	Only system administration can edit	Always available	This is general information provided by the interface of the system. It is available for those who need to create an account, use the system, and read general information about the system. Also, if the user has some questions, they can contact the system's customer services.

The number of parking floors available		Only available to System Administration and individual, local authority			The system administrator can add a new floor that makes more spots to increase the user's number. The spot number is based on the space in the place and the system administration adds an entrance/exit panel based on the working hours of the organisation. For example, there are two parking floors, and each floor has 12 parking spots. The parking spots are available

					from 8:00am to 8:00pm. The user can find an available parking spot on each floor and make payments every hour for the parking. If the floor or the parking spots are undergoing maintenance work, the system administration will modify the parking system so that they appear as unavailable parking spots in the system for users.

Parking Permit ID	local authority	Only available to council, building owner and project owner	local authority can edit	Always available	This permit ID should be issued by the local council.
Personal Information for users of the parking facility	Individual	Only available to individual and system administration	Only modifiable to individual	Always available	To find parking spots, the user should create an account and fill in the user's information (first name, last name, email, phone number, student ID or staff ID, age). After that, the user can access the app to find a parking spot. The user can't find a parking spot without registering for the parking

					system. The user's information is protected and can't be seen by either the system administrator or other users. When the user selects a parking spot, the system will record their username, the parking spot and the parking floor so that the system administrator can track the system and read this information. Also, the users can edit their information in the system.

List of Parking Violations	Police officer	Only available to individual and police officer	Only police officer can edit	Always available (paid, unpaid)	The system notifies the police of any parking violation. If an unauthorised driver parks in a disabled area or a prohibited area, a message will be sent to the police to take the appropriate action.

Table *2*: Attendance management system access control

Data Description	**Data Controller**	**Confidentiality Restriction**	**Integrity Restrictions**	**Availability Restrictions**	**Notes**
• Attendance Management System General Information • Operator Contact	System Administrator	Available to everyone	Only system administration can edit	Always available	This is general information in the interface of the system. It is available for those who need

information					to create an account, use this system, and read general information about the system. Also, if the user has any questions, they can contact the system's customer service.
Number and information about the students (who is an available in the system)		Only available to System Administration and individual, local authority			System administrator can add a new student based on the student's timetable.
Personal Information of each student	Individual	Only available to individual and system administration	Only modifiable to individual	Always available	To record attendance, the student should put

					their finger on a device. The user's personal information is kept confidential. The administrator can only see their name and the classes they attended.

Table 3: Access door system access control

Data Description	**Data Controller**	**Confidentiality Restriction**	**Integrity Restrictions**	**Availability Restrictions**	**Notes**
• Access Door System General Information • Operator Contact information	System Administrator	Available to everyone	Only system administration can edit	Always available	This information is general information in the interface of the system. It is available for those who need to create

					an account who can use this system and read the general information about the system. Also, if the user has some questions, they can contact the system's customer service.
The number of Doors		Only available to System Administration and individual, local authority			System administrator can add new Door to the system.
Personal Information for users of the access door	Individual	Only available to individual and system administration	Only modifiable to individual	Always available	To access the door, users should pass their card on the device. The user's

					personal information is kept confidential. The administrator can only see their name and the classes they attended.

Table 4: Smart conditioning system access control

Data Description	Data Controller	Confidentiality Restriction	Integrity Restrictions	Availability Restrictions	Notes
• Smart Office System General Information • Contact information	System Administrator	Available to everyone	Only system administration can edit	Always available	This is general information in the interface of this system. It is available for those who need to create an account, who can use this system

					and read the goals of the system. Also, if the user has any questions, they can contact the system's customer service.
The number of air conditioning		Only available to system administration			The system administrator can add and identify a new office smart air conditioning.
Personal Information for users of Smart conditioning system access control	Individual	Only available to individual and system administration	Only modifiable to individual	Always available	To control the air conditioning, users should use their staff ID. The user's personal information is kept

					confidential. The administrator can only see data regarding the systems they administer.

Appendix C: Competency questions

Table 1: IoT devices competency questions

Competency questions	**Linked case study**
What building and physical location within a building, is a given sensing device associated with?	All scenarios
How many sensor devices does a given space have?	All scenarios
What is the name and location of the building that a particular parking space serves?	Smart parking
Who are the organisations that supply parking spaces to an actor?	Smart parking
What is the name and location of the classroom that has an attendance recording system?	Attendance management
Who are the organisations that supply attendance recording to an actor?	Attendance management
What is the name and location of the building that a particular secure door controls access to?	Physical access control
What are the organisations that supply physical access control to an actor?	Physical access control
Who are the actors that supply physical access control to an actor?	Physical access control
What is the name and location of the space that a particular air conditioning control unit serves?	Smart conditioning
What are the organisations that supply air conditioning control to an actor?	Smart conditioning
Who are actors that administer air conditioning control for a given space?	Smart conditioning

What sensor devices monitor air conditioning in a given space?	Smart conditioning
What is the physical location of a given air conditioning system?	Smart conditioning

Table 2: Built environment data format competency questions

Competency questions	**Linked case study**
How many parking spaces does a given building have?	Smart parking
What sensor devices monitor a given parking space?	Smart parking
What is the physical location of a given parking space?	Smart parking
What is the total parking space capacity of given location?	Smart parking
What is the total free parking space capacity of a given location at a given time?	Smart parking
Is a particular parking space suitable for disabled users?	Smart parking
What sensor devices monitor a space as part of a given attendance system?	Attendance management
What is the physical location of a specific attendance recording system?	Attendance management
What is the total number of attendance recording systems in a given location?	Attendance management
How many access-controlled doors does a given building have?	Physical access control
What sensor devices monitor a given secured door?	Physical access control
What is the physical location of a given access-controlled door?	Physical access control

How many smart air conditioning units does a given space have?	Smart conditioning
How many smart air conditioning units does a given building have?	Smart conditioning

Table 3: Actor competency questions

Competency questions	**Linked case study**
What information is held about a given student?	All scenarios
What information is held about a given staff member?	All scenarios
Which actors can utilise a given parking space?	Smart parking
What information is held about a given parking officer?	Smart parking
Who are the actors that administer a given parking space?	Smart parking
Which actors can utilise a given attendance recording service?	Attendance management
Who are the actors that administer attendance recording services?	Attendance management
Which actors can open a given security door?	Physical access control
Which actors can control a given smart air conditioning?	Smart conditioning

Table 3: Built environment services competency questions

Competency questions	**Linked case study**
What are the details of the service that manages the smart parking system at a given location?	Smart parking
Identify all of the smart parking services that require authentication?	Smart parking
What parking violations have been issued to a given actor across all parking sites?	Smart parking

How many violations has a given parking officer issued and at what sites?	Smart parking
What is number of uses per day of a given parking space and their timestamps?	Smart parking
What student actors attended a given class?	Attendance management
What timestamps a student entering a class?	Attendance management
What are the details of the service that manages attendance at a given location?	Attendance management
What are the details of the service that manage the physical access control system at a given location?	Physical access control
What timestamps an actor controlled physical access?	Physical access control
What are the details of the service that controls the smart air conditioning system at a given location?	Smart conditioning
What timestamps an actor controlled smart conditioning?	Smart conditioning

Table 4: Security standards competency questions

Competency questions	**Linked case study**
Who are the actors that are authorised to use a given service?	All scenarios
Does a given actor have access to book a parking space?	Smart parking
Does a given actor have access to record a violation?	Smart parking
Does a given actor have access to display a given violation?	Smart parking

What are the access control policies that govern the access rights of an actor?	Smart parking
At what timestamps does an authorised user access a restricted service?	All scenarios
What are the access control policies governing the reservation of a parking space service?	Smart parking
What are the access control policies governing the issue of violations on a parking space service?	Smart parking
What are the access control policies regarding displaying violations for a given parking space service?	Smart parking
Does a given actor have access to an attendance recording system?	Attendance management
What are the policies assigned to a given actor?	Attendance management
What are the policies governing an attendance recording service?	Attendance management
Does a given actor have access to a physical access control system?	Physical access control
What are the policies that govern a given physical access control service?	Physical access control
Does a given actor have access to an access smart conditioning system?	Smart conditioning
What are the policies that govern an air conditioning control service?	Smart conditioning
Which actors can control a given smart air conditioning system?	Smart conditioning

Appendix D: Re-engineering of built environment non-ontological resources

1. class diagrams

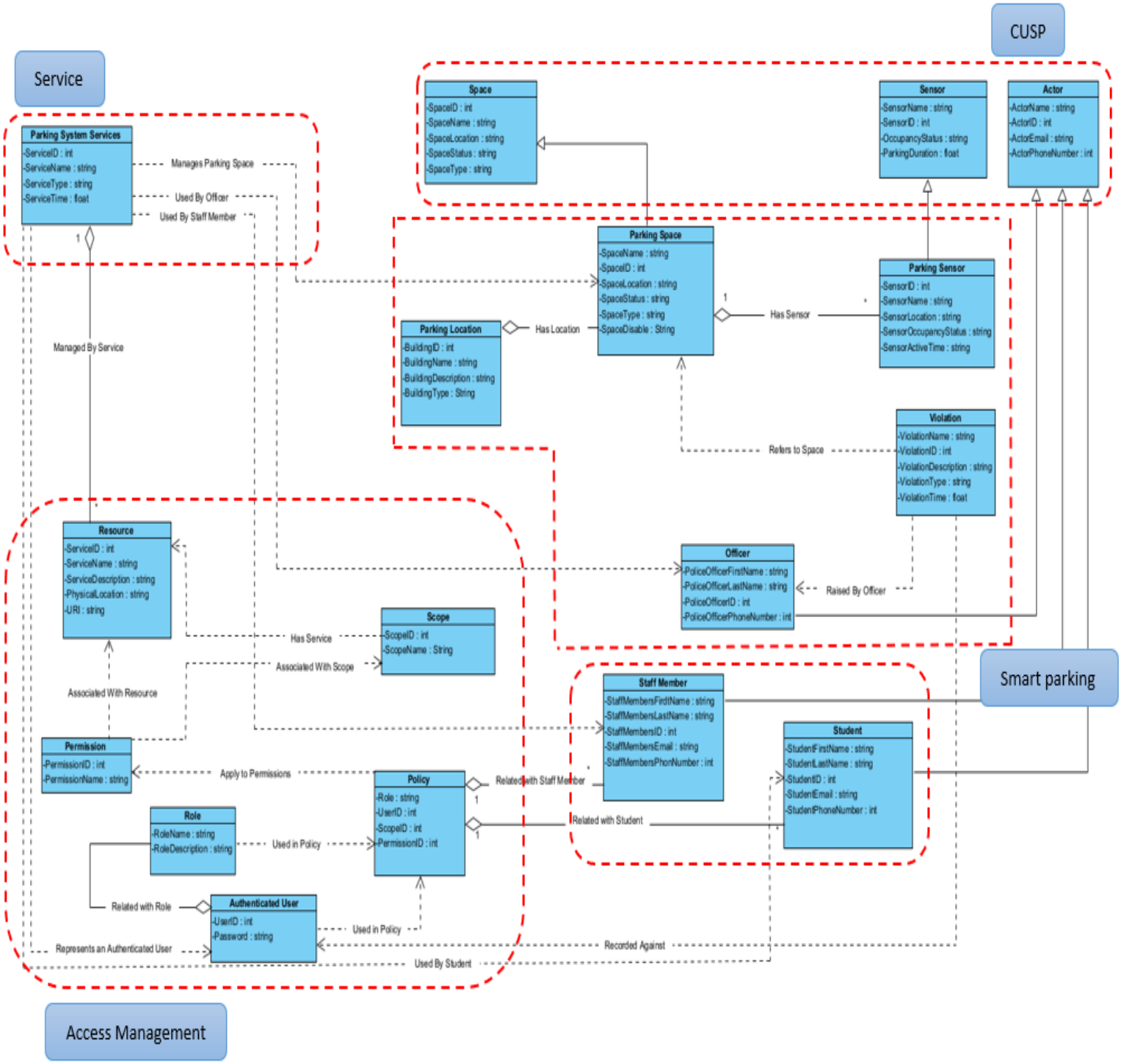


Figure 1. Smart parking system access control

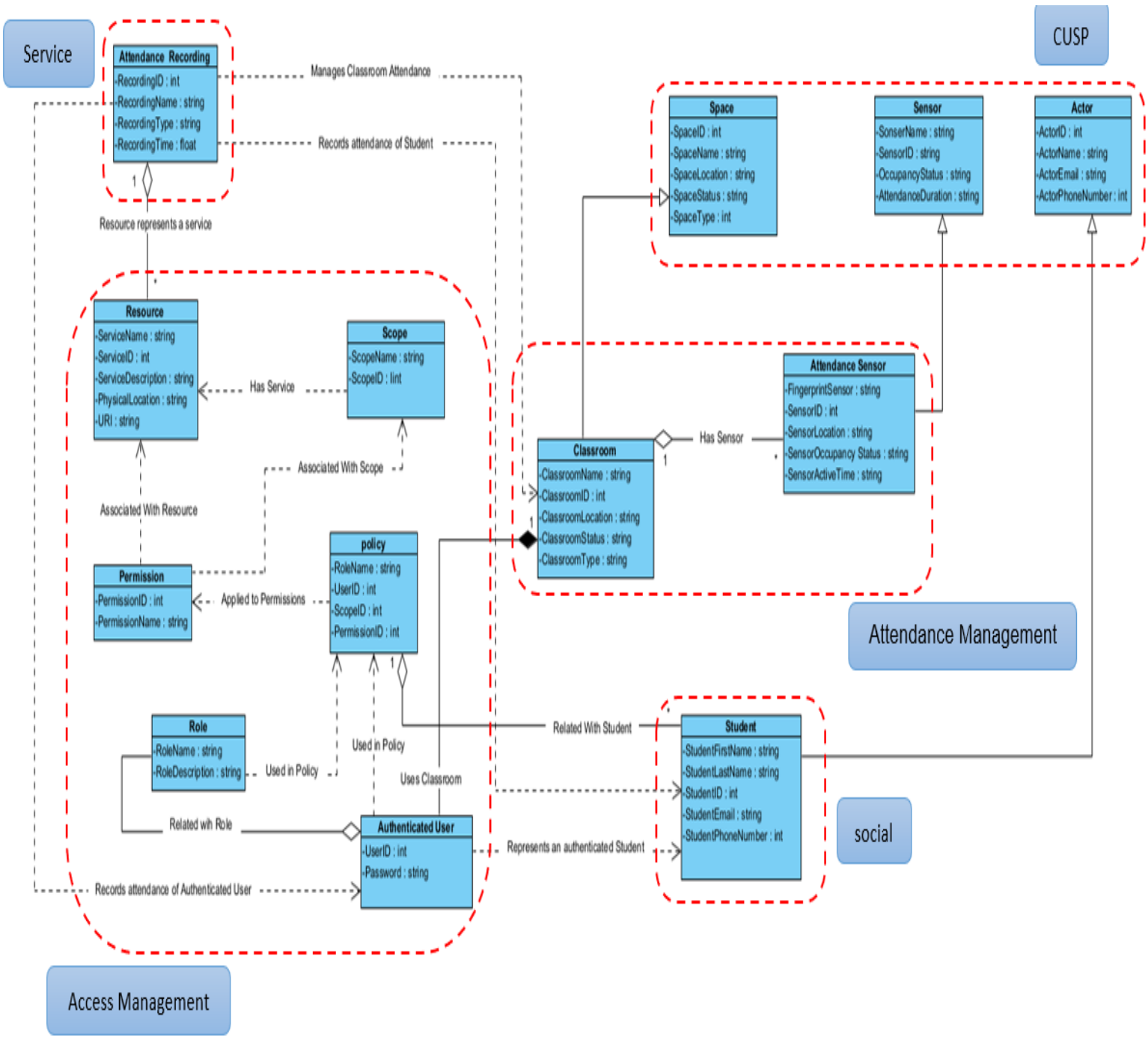


Figure 2. Attendance management system access control

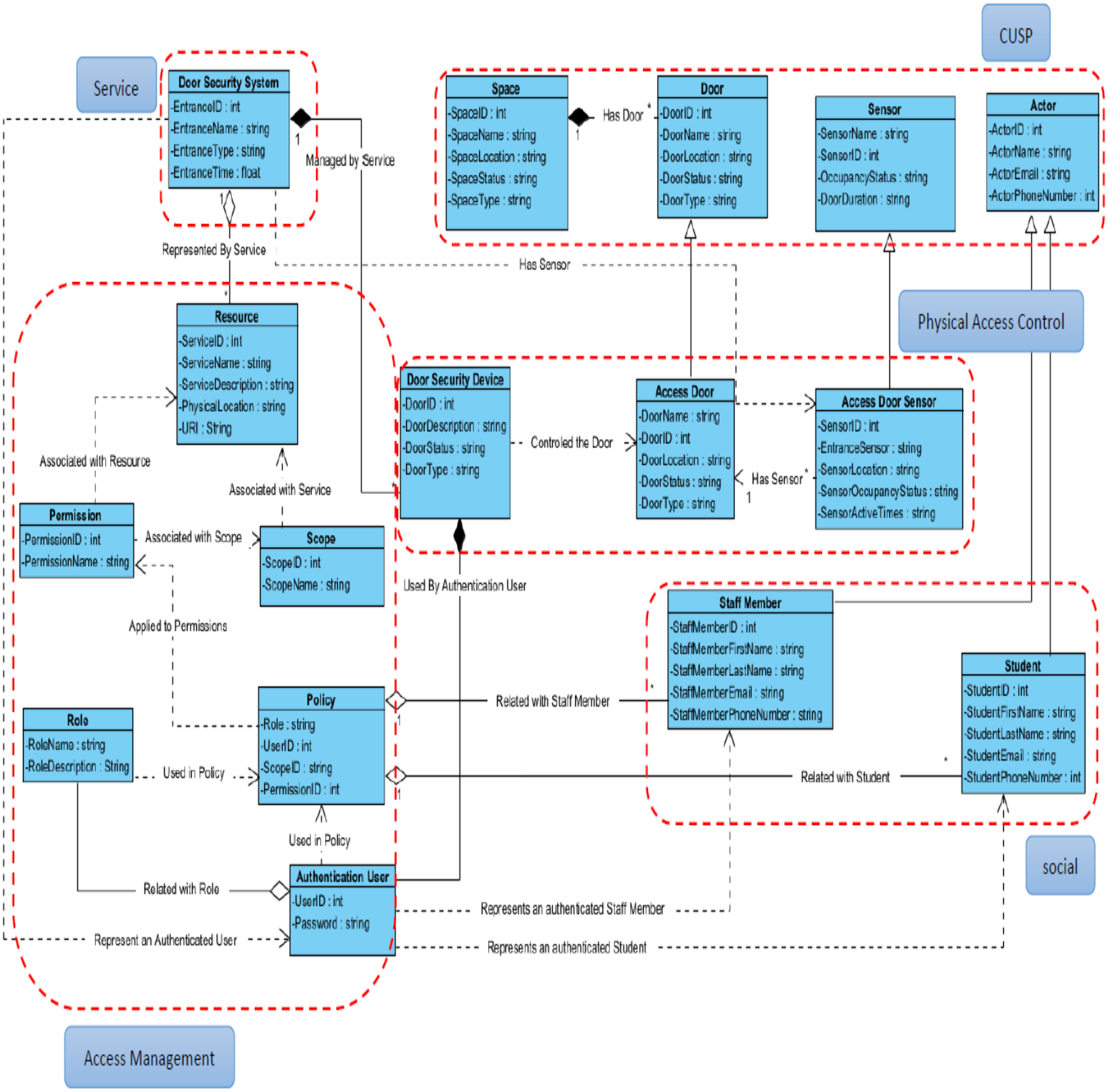


Figure 3. Access door system access control

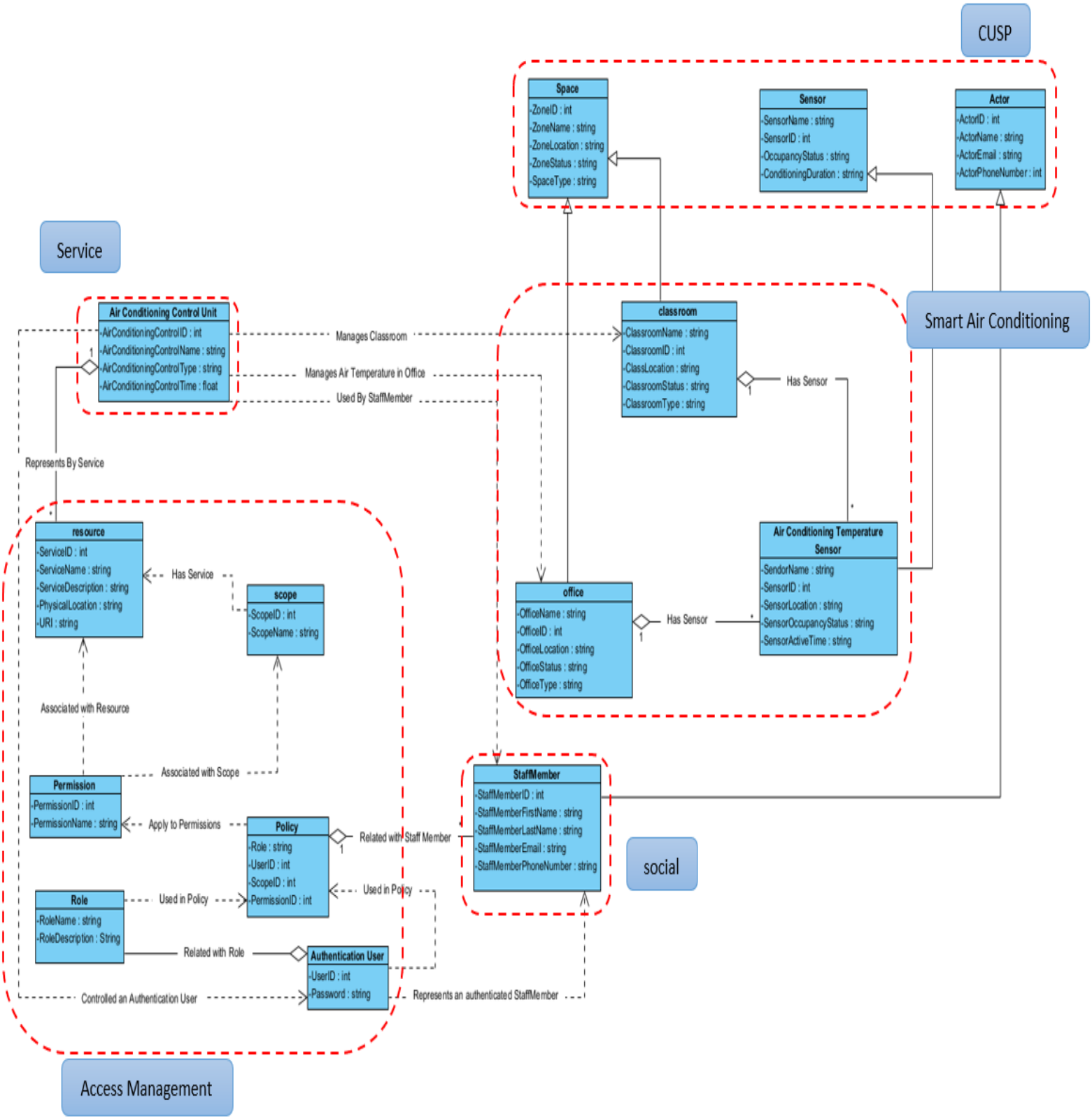


Figure 4. Smart conditioning system access control

2. Individuals for smart parking use case

Table 1: Individuals for smart parking use case

Individual Name	**Class**	**Data Properties**	**Object Properties**	**Notes**
Space 10	Parking Space	Name Occupancy status	**hasSensor**('Space 10 Sensor 10') **hasLocation**('Queens's Building')	
Space 10 Sensor 10	Parking Sensor	ID	**hasSensor** ('Space 10')	
Reservation of Parking Space Permission	Permission	Name	**AssociatedWithResource**(' Reservation of Parking Space Service')	
Recording of Parking Violation Permission	Permission	Name	**AssociatedWithResource** ('Recording of Parking Violation Service')	Inverse of AssociatedWithResource("Recording of Parking Violation)
Displaying Parking Violation Permission	Permission	Name	**AssociatedWithResource** ('Displaying Parking Violation Service '**)**	Inverse of AssociatedWithResource("Displaying of Parking Violation)
Reservation of Parking Space Permission	Permission	Name	**AssociatedWithScope**(' Reservation of Parking Space Service')	
Recording of Parking	Permission	Name	**AssociatedWithScope** ('Recording	

Violation Permission			of Parking Violation Service')	
Displaying Parking Violation Permission	Permission	Name	**AssociatedWithScope** ('Displaying Parking Violation Service'**)**	
Reservation of Parking Space Service	Smart parking Service, Resource	URI	**ManagesParkingSpace**(' Space10')	
Recording of Parking Violation Service				
Displaying Parking Violation Service				
Parking penalty No #157	Violation	Description	**RasiedByOfficer**(' Khalid')	
			RecordedAgainst(' Sara')	
			RefersToSpace(' Space 10')	Inverse of RefersToSpace

				(Violation, Parking Space)
Sara	Student, Authenticated User	Name	**RelatedWithRole** (‘ Reservation of Parking Space Policy’)	
Ahmed	Staff Member, Authenticated User	Name	**RelatedWithRole** (‘Reservation of Parking Space Policy’’)	
Khalid	Police Officer, Authenticated User	Name	**RelatedWithRole** (‘Recording of Parking Violation Policy’’) **RelatedWithRole** (‘Displaying Of Parking Violation Policy’’**)**	
Allow Authenticated User (Student) Allow Use of Parking Facility Reservation	Policy	Name	**RelatedWithPermission** (‘Reservation of Parking Space’’)	
Allow Authenticated User (Staff member) Allow Use of	Policy	Name	**RelatedWithPermission**(‘ Reservation of Parking Space’’)	

Parking Facility				
Allow Authenticated User (Police officer) Allow Use of Parking Violations	Policy	Name	**RelatedWithPermission** (‘Recording of Parking Violation’’) **RelatedWithPermission** (‘Displaying Parking Violation’’)	

Appendix E: Access management ontology

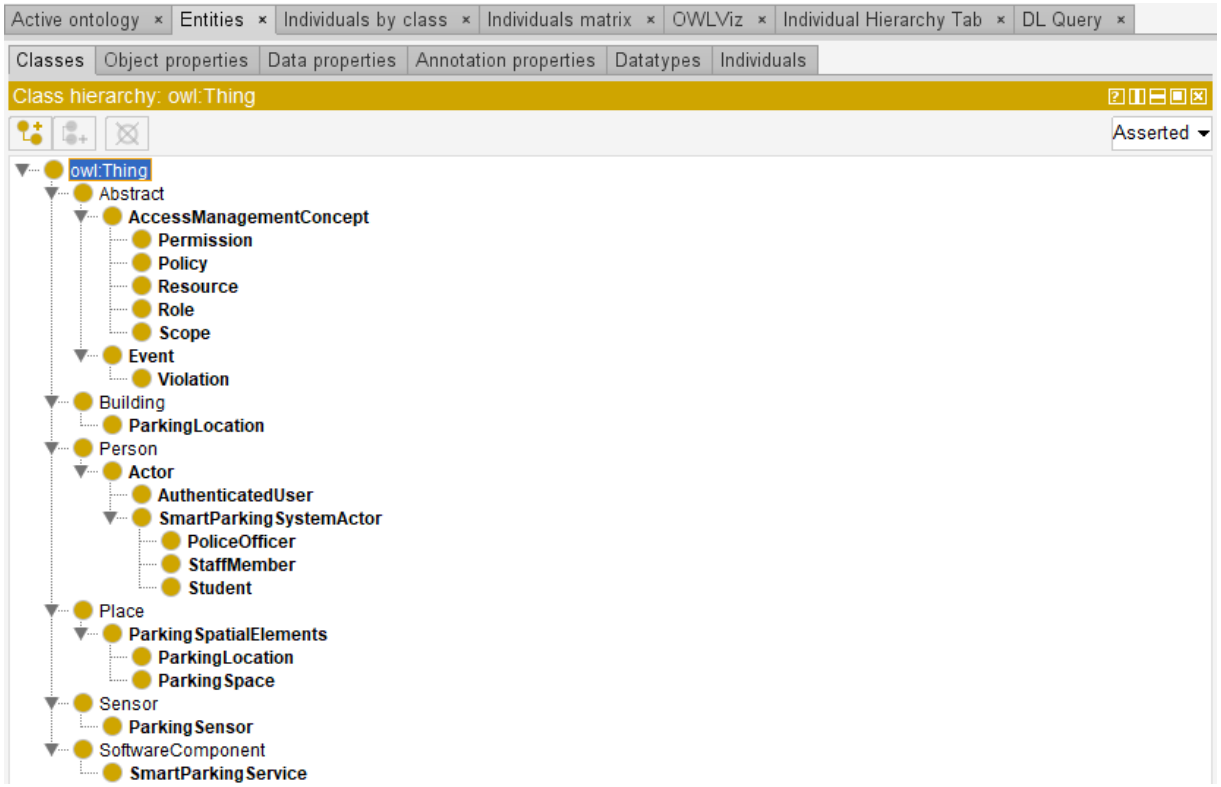


Figure 1 Classes Related to the Smart Parking Case Study

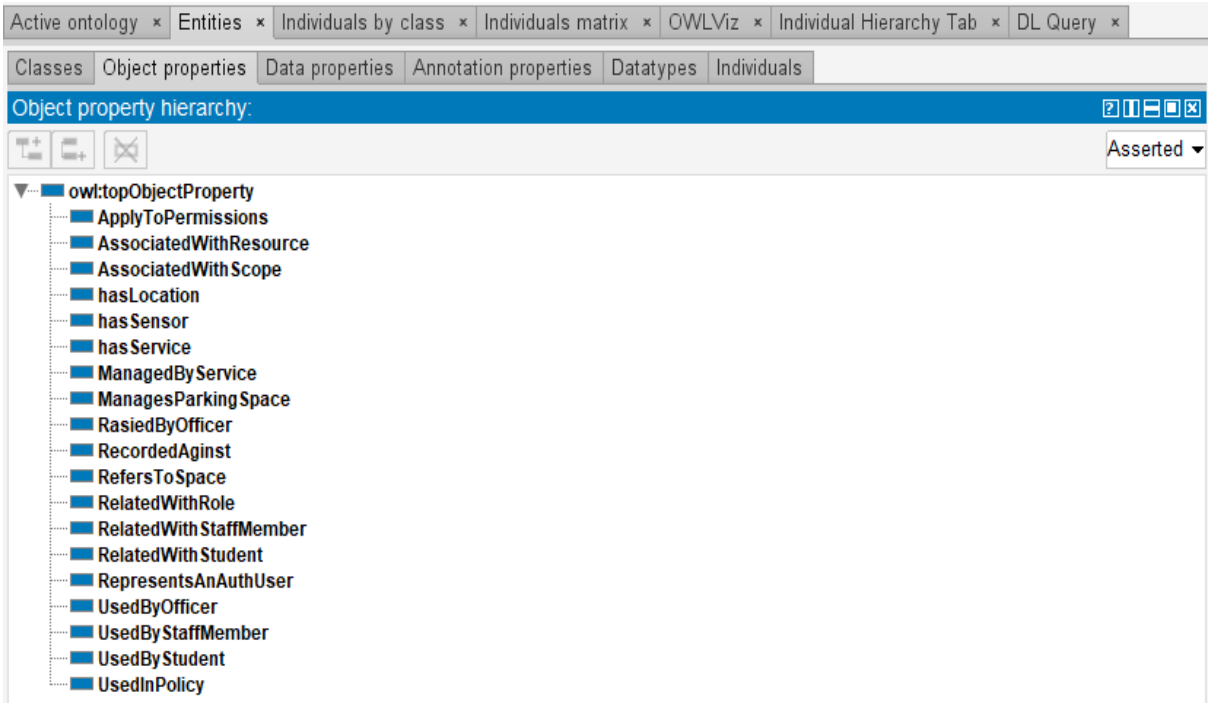


Figure 2. Object properties used in Smart Parking Case Study

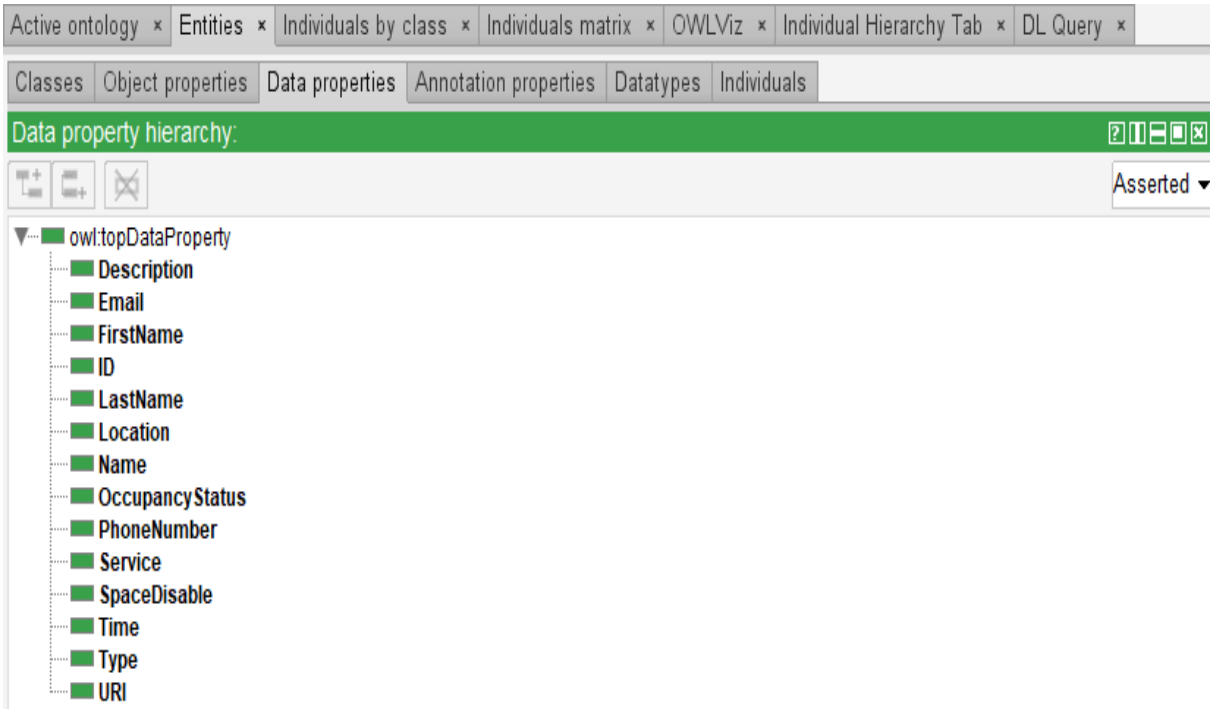


Figure 3. Data properties within the smart parking Case Study

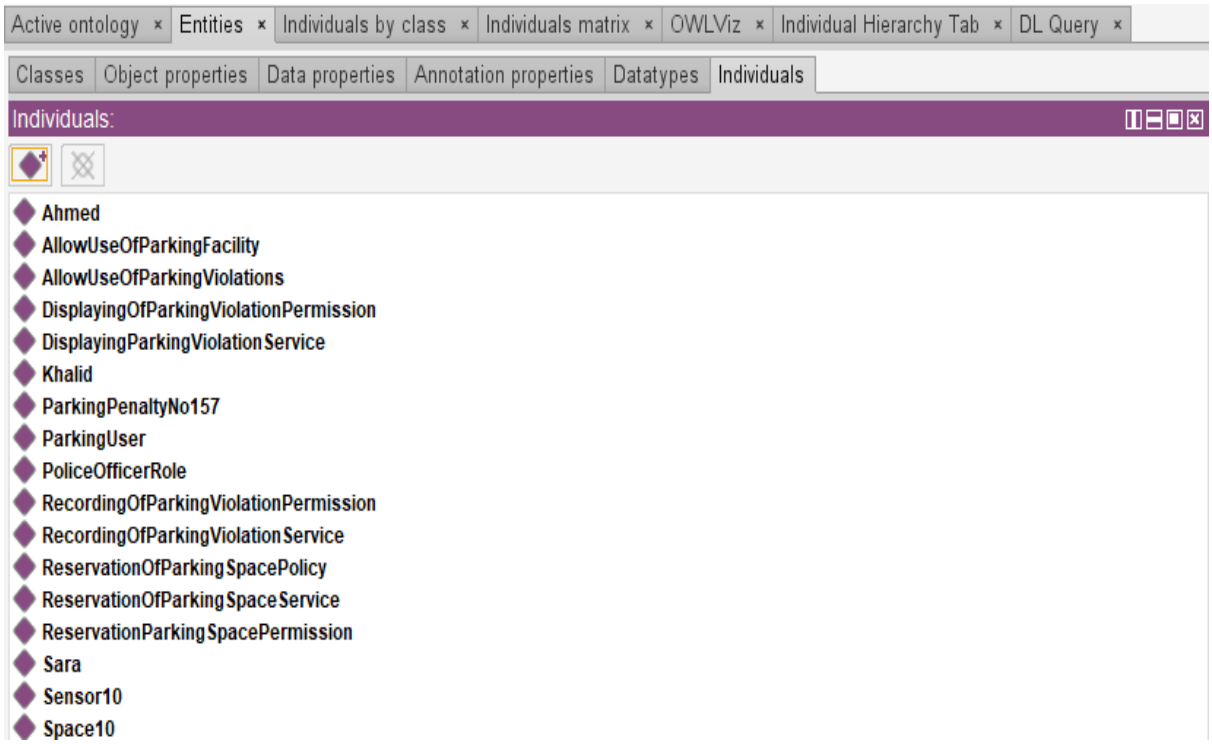


Figure 4. Individuals utilised within the smart parking Case Study

Appendix F: Competency question verification

Table 1: Competency question verification

Competency Question	**Response**
What building, and physical location within a building, is a given sensing device associated with?	This has been met through the implementation of the Space class and the hasLocation object property that relates it to the Sensor class. This is provided by existing CUSP ontologies.
What is the name and location of the classroom that has an attendance recording system?	This has been met through the implementation of the Space class, isConstituentOf object property. This is provided by existing CUSP ontologies however a new class to represent attendance monitoring system was created.
Who are the organisations that supply attendance recording to an actor?	This has been met through the implementation of the Attendance Recording Service class, hasOrganisationOwner object property. This is provided by existing CUSP ontologies however a new class to represent attendance monitoring system was created.
What is the name and location of the building that a particular secure door controls access to?	This has been met through the implementation of a SecureDoor subclass of the existing Door class and hasLocation object property in Physical Access Control ontology.
Who are the organisations that supply Physical Access Control to an actor?	This has been met through the implementation of the Physical Access Control Service class, hasOrganisationOwner object property. This was a newly added concept in the Service ontology.
Who are the actors that supply Physical Access Control to an actor?	This has been met through the implementation of the System Actor class, RelatedWithRole

	object property in the newly created additions to the Social ontology.
What is the name and location of the space that a particular air conditioning control unit serves?	This has been met through the implementation of the Office class (a new subclass of Space) and the hasLocation object property in the Smart Air Conditioning ontology.
Who are the organisations that supply air conditioning control to an actor?	This has been met through the implementation of the Air Conditioning Control Service class, and the hasOrganisationOwner object property newly created in the Service ontology.
Who are actors that administer air conditioning control for a given space?	This has been met through the implementation of the Actor class, RelatedWithRole object property in the Social ontology.
What sensor devices monitor air conditioning in a given space?	This has been met through the implementation of the Office class, hasSensor object property in the Smart Air Conditioning ontology.
What is the physical location of a given air conditioning system?	This has been met through the implementation of the Office class, hasLocation object property on the Airconditioning Sensor system.
What sensor devices monitor a space as part of a given attendance system?	This has been met through the implementation of the Classroom class (a subclass of Space) and its hasSensor object property in the Attendance Management ontologies.
What is the physical location of a specific attendance recording system?	This has been met through the implementation of the Space class and its hasLocation Classroom object property in CUSP ontology.
What is the total number of attendances recording systems in a given location?	This has been met through the implementation of the Classroom class, isConstituentOf object property in the Attendance Management

	ontologies. Following the processing performed by the attendance monitoring the total attendance can be calculated using the totalAttendance data property. This is attached to the “TimeTableEvent” class which is associated with a given space using a “takesPlaceIn” object property.
How many access-controlled doors does a given building have?	This has been met through the implementation of the Security Door class, isConstituentOf object property in the Physical Access Control ontologies.
What sensor devices monitor a given secured door?	This has been met through the implementation of the Security Door class (subcass of door) and its hosts object property in Physical Access Control ontology.
What is the physical location of a given access-controlled door?	This has been met through the implementation of the Security Door class and its hasLocation object property in Physical Access Control ontology.
How many smart air conditioning units does a given space have?	This has been met through the implementation of the Office class (subclass of Space) and its isConstituentOf object property in the Smart Air Conditioning.
What is information is held about a given student?	This has been met through the implementation of the Student class (subclass of actor). This class has the following data properties; First name, Last name, Email and phone Number Data. These have been added to the social ontology.
What is information is held about a given staff member?	This has been met through the implementation of the Staff Member class (subclass of Actor). This class has the following data properties;

	First name, Last name, Email and phone Number.
What student actors, attended a given class?	This has been met through the implementation of the Student class. Following the processing performed by the attendance monitoring links are established using the studentAttended object property between the “TimeTableEvent” class and the Student Class.
At what timestamps did a student enter a class?	This has been met through the implementation of the Student class. Following the processing performed by the attendance monitoring links are established using the attended object property between the “TimeTableEvent” class and the Student Class.
What are the details of the service that manages attendance at a given location?	This has been met through the implementation of the Classroom class, and the hasService object property that links it to the service that manages the attendance recording
What are the details of the service that manage the Physical Access Control system at a given location?	This has been met through the implementation of the Door class, and the hasService object property that links it to the service that control the access door
At what timestamps did an actor open a secured door?	This has been met through the implementation of the Actor class. Following the processing performed by the access door service links are established between the door using the object property between the “accessTimestamp” class and the Actor Class.
What are the details of the service that control the smart air conditioning system at a given location?	This has been met through the implementation of the Air Conditioning Control Service class, hasService object property in the Service ontologies.

What timestamps an actor controlled a Smart Conditioning?	This has been met through the implementation of the Policy class, i ApplyToPermissions Can Air Conditioning Control object property in the Access Management ontologies.
At what timestamps does an authorised user access the air conditioning service service?	This has been met through the implementation of the StaffMember class. Following the processing performed by the air conditioning service links are established using the control object property between the “TimeTableEvent” class and the StaffMember Class.
Who are actors that are authorised to use a given service?	These have been implemented through the use of the Policy, Actor, Role, Permission, and Resource Classes. These classes allow the definition of a set of flexible permissions. An actor is (optionally) assigned to a role. At the same time resources (services or physical devices) provide. permissions that conceptualise what functionality that they can perform. Then a policy provides a mapping between user/role and permissions for a given resource.
Which actors can utilise a given attendance recording service?	
Who are actors that administer attendance recording services?	
Which actors can open a given security door?	
Which actors can control a given smart air conditioning?	
Does a given actor have access to a record a violation?	
Does a given actor have access to a display a given violation?	
What are the access control policies that govern the access rights of an actor?	
Does a given actor have access to an attendance recording system?	

What are policies assigned to a given actor?	
What are policies governing an attendance recording service?	
Does a given actor have access to a Physical Access Control system?	
What are policies that govern a given Physical Access Control service?	
Does a given actor have access to an access smart conditioning system?	
What are policies that govern given an air conditioning control service?	
Which actors can control a given smart air conditioning system?	

Appendix G: CUSP access control ontology

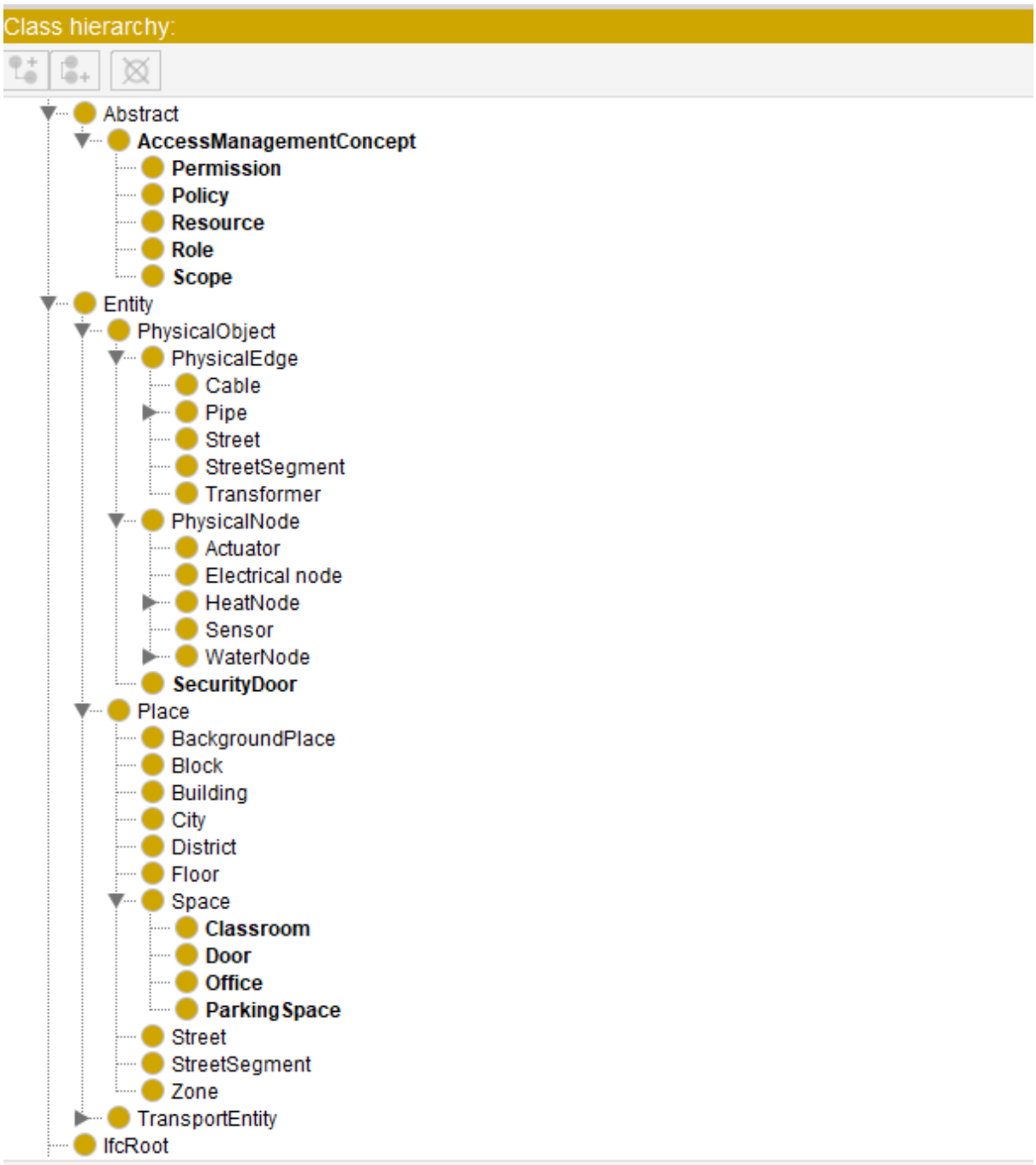


Fig 1. CU class

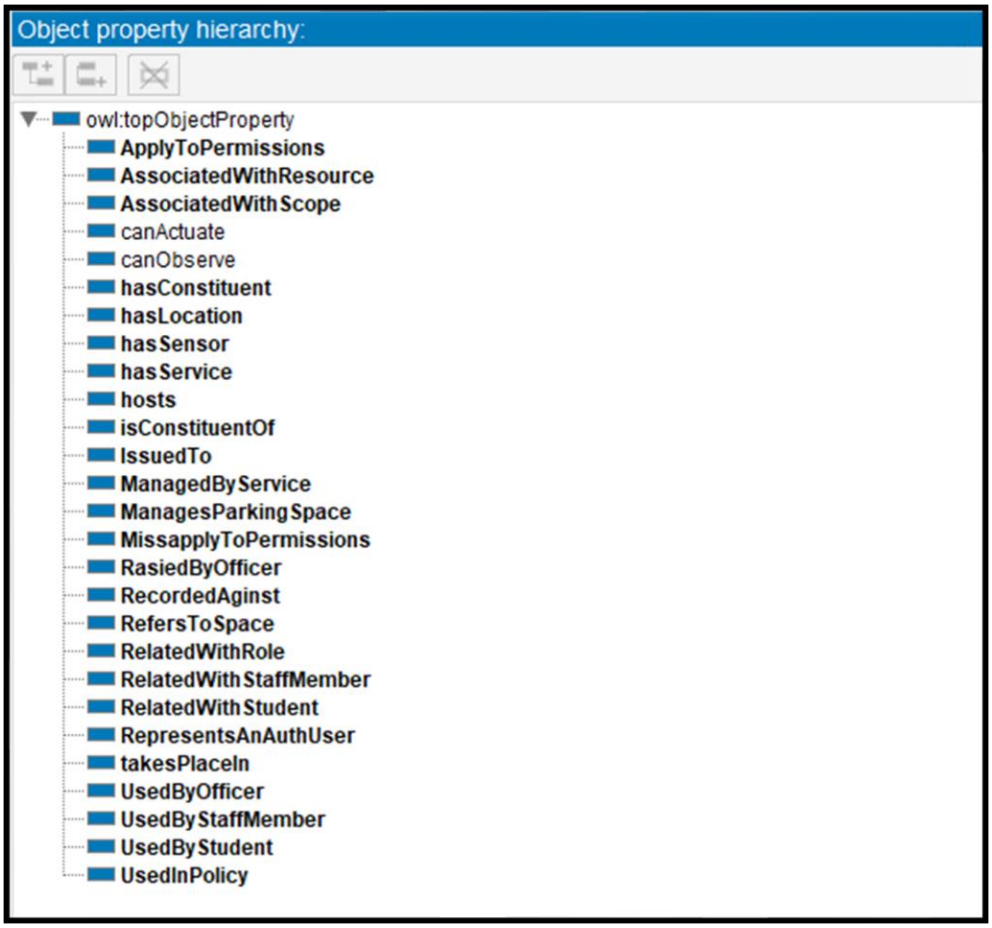


Fig 2. CU object property

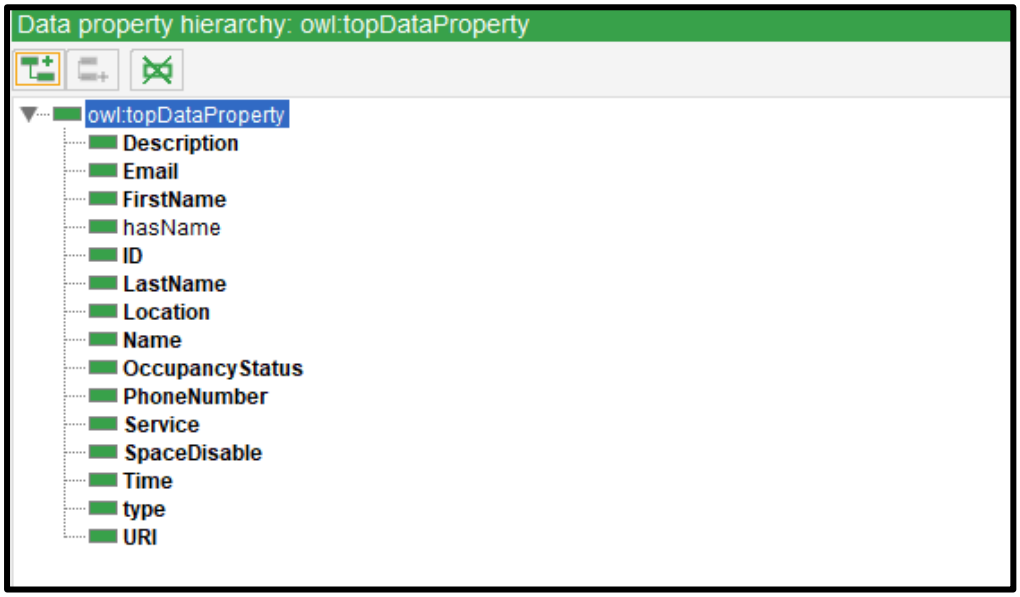


Fig 3. CU data property

Appendix H: Conferences and skills

International Conference on Engineering, Technology and Innovation (ICE-IEEE-TEMS 2021)

Cardiff University
Engineering
Kaznah Alshammari
17 Admiral House, 38-42 Newport Rd
Cardiff
CF24 0DH
United Kingdom

Cardiff University
Professor Yacine Rezgui
School of Engineering
Queen's Buildings - South Building
5 The Parade, Newport Road
Cardiff
CF24 3AA
United Kingdom

Cardiff, 08/Nov/2021

To Whom It May Concern

This is to confirm that **Kaznah Alshammari** is welcome to participate in **27th ICE IEEE ITMC 2021 Conference**, to be held in Cardiff, June 21-23, 2021.

Please note that registration fees,will not be supported by the conference organizers.

Kaznah Alshammari is author/co-author of the following accepted contribution(s):

Industry Engagement for Identification of Cybersecurity Needs Practices for Digital Twins
Author(s): Alshammari, Kaznah; Beach, Thomas; Rezgui, Yacine
Presenting Author: Alshammari, Kaznah
Submission Type / Conference Track: Engineering
Status: Finalized

We look forward to seeing Kaznah Alshammari.

With kind regards,

ICE 2021 Organizing Committee
Local Organizer of the Conference

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

Cardiff University

CERTIFICATE *of* ATTENDANCE

THIS ACKNOWLEDGES THAT

Khaznah Magbel Alshammari

Has successfully attended

The scientific workshop entitled

'How to be succeed in PhD journey'

Organised by

Cardiff University Students' Union- Saudi Society

On 13 April. 2019