An Authorisation Framework using Building Information Models

Nimalaprakasan Skandhakumar, Jason Reid, Ed Dawson,
Robin Drogemuller and Farzad Salim

Queensland University of Technology, Queensland, Australia
Email: {n.skandhakumar,jf.reid,e.dawson,robin.drogemuller,f.salim}@qut.edu.au

A Building Information Model (BIM) is an electronic repository of structured, three-dimensional data that captures both the physical and dynamic functional characteristics of a facility. In addition to its more traditional function as a tool to aid design and construction, a building information model can be used throughout the lifecycle of a facility, functioning as a living database that places resources contained within the building in their spatial and temporal context. Through its comprehension of spatial relationships, a BIM can meaningfully represent and integrate previously isolated control and management systems and processes, and thereby provide a more intuitive interface to users. By placing processes in a spatial context, decision-making can be improved, with positive flow-on effects for security and efficiency. In this article, we systematically analyse the authorisation requirements involved in the use of building information models. We introduce the concept of using a building information model as a graphical tool to support spatial access control configuration and management (including physical access control). We also consider authorisation requirements for regulating access to the structured data that exists within a BIM as well as to external systems and data repositories that can be accessed via the BIM interface. With a view to addressing these requirements we present a survey of relevant spatiotemporal access control models, focusing on features applicable to building information models and highlighting capability gaps. Finally, we present a conceptual authorisation framework that utilises building information models.

Keywords: Access Control; Authrorisation Models; Building Information Model

Received 00 January 2009; revised 00 Month 2009

1. INTRODUCTION

Building Information Models (BIM) are used in the fields of building design, construction and facility management. Traditionally, their main application has been in facilitating information exchange, using a virtual representation of the building that is a direct analogue of the physical structure, among different stakeholders engaged in building design and construction. More recently, there has been recognition of the potential value of using a BIM after a building is commissioned as a tool to manage the facility and the increasingly complex processes that occur within it [1]. In this setting a BIM can act as a graphical 'front end' or portal to provide integrated access to a range of complex but currently independent subsystems that are essential to the operation of a modern facility. These include Heating, Ventilation, and Air Conditioning (HVAC) control systems, asset management, fault handling and maintenance systems, fire control systems, Closed Circuit Television (CCTV) monitoring systems and Physical Access Control Systems (PACS). To understand the benefits of integration consider the following scenario: an operator is notified of a malfunctioning pump via a graphical display on a three dimensional building map. The interface immediately gives them the option of remotely shutting down the pump - a step which requires interaction of the BIM with the HVAC control subsystem. A CCTV camera feed from the plant room automatically appears allowing the operator to view the affected area for intruders or damaging leaks. Further, they are able to check the warranty status of the pump and raise a service request with the supplier. This step requires interaction with the asset management subsystem. BIM-based integration offers efficiency gains because the operator no longer needs to independently locate and interact with the object of interest through multiple 'stove-piped' systems. Moreover, the actions required to respond to the event can be formalised as a step-by-step process or *workflow* that is managed in an integrated way through the BIM. We argue that recent

proposals [1] to use a BIM in this way introduce complex security challenges. In particular, an overarching authorisation system is required to ensure that this powerful monitoring and control capability is only available to users possessing appropriate authority. The need to maintain security in an integrated way is becoming a high priority with the ever-increasing reliance on information and communications technology across all aspects of facilities operation. This need is particularly pressing in facilities that are exposed to complex threats such as ports and airports, chemical manufacturing plants, defence facilities, power stations and the like.

1.1. Authorisation for BIM

The term *authorisation* refers to a security service and related processes that grant or deny requests made by authenticated users to access *resources* according to *rules* (also referred to as a *security policy*). Authorisation encompasses both *authentication* (are users who they say they are?) and *access control* (should ta user's requests to access a resource be granted?). Some authors distinguish authorisation from access control (i.e., access decision making) [2]. When this distinction is drawn, authorisation refers to the formulation of access policy, which allocates access rights to users, and access control is the enforcement of the policy via allow/deny responses to access requests. In this article, we take the more common approach of using both terms interchangeably.

We use the term *logical access control* to refer to the service that regulates access to resources that take the form of information and information services. Examples of information include: the BIM elements themselves (i.e. *BIM content* - the structured objects that represent walls, wiring, pipes etc.) and information that is generated or stored outside the BIM but made accessible through it e.g., digital CCTV footage or the operational status of a pump (made available via a HVAC control system). An example of an information service is a function within an asset management system that initiates and subsequently manages the lifecycle of a maintenance request for a faulty piece of equipment. In contrast, and consistent with its widely understood meaning, we use the term *physical access control* to refer to the service that regulates human access to *spaces* within a facility. One of the goals for our BIM authorisation architecture is to unify logical and physical access control within a single cohesive framework.

The distinction that we have drawn between resources that are BIM-internal and BIM-external reflects two distinct access control contexts that a BIM authorisation framework must address: it must be capable of enforcing security policies with respect to the BIM content as well as regulating access to resources accessed via the BIM but external to it. We will briefly introduce each of these aspects in turn and consider them in more detail in Section 4.

Controlling access to BIM content is important, because different elements and spaces within the model are subject to different access rules. Much of the information in a BIM may be operationally sensitive so users should only have access when they have a legitimate 'need to know'. For example, the details of the critical network wirings need not be visible to an air-conditioning maintenance operator. Thus, the visualisation of a building information model needs to be controlled based on the role, assigned tasks (and possibly other contextual factors such as time and location) of the user. This authorisation capability also needs to be included in BIM tools such as design analysis tools, model servers, and BIM viewers.

Authorisation for the BIM-external case is more challenging. The usage scenario we are interested in involves the use of BIM as a unifying 'front end' to a range of disparate systems each of which may also have its own authorisation system. For example, the HVAC system may have its own database of users and their associated roles (maintenance engineer, control room operator etc.) which determine the operations they can perform. If a control room operator is accessing the HVAC system through the BIM, the two authorisation services must be able to cooperate to enforce the security policy. Ideally, the two systems would leverage an enterprise-wide identity and access management framework which would avoid the need to manage duplicate user databases for each application. Integration of the authorisation systems of the BIM and associated subsystems presents a range of challenges which we examine in greater detail in later sections.

1.2. Spatial authorisation

The demand for spatially aware access control systems has increased in the past decade with the widespread adoption of location-based services [3]. Many new application scenarios have emerged that use geospatial data organised in different thematic layers representing different aspects of the application domain [4].

A key advantage of using a BIM to support authorisation is that it allows an organisation to define and *reliably* enforce access control policies that have a spatial dimension - a powerful capability that is currently not delivered. For example, an organisation may have a policy that only Human Resource staff can access the part of the building where sensitive HR records are stored (the 'Restricted HR zone'). The PACS administrator implements this policy by manually identifying the access controlled doors that give access to this space and configuring the physical access control system (PACS) to give HR staff access to each affected door. Because currently available physical access control systems have no spatial awareness, there is no way to express the concept of 'Restricted HR Zone'

other than as a set of door identifiers. If the space is remodelled, this configuration must be changed and a different set of doors may be affected but again, they need to be manually identified and there is ample room for error, particularly in large and complex facilities.

If the PACS is integrated with a BIM, the zones can be graphically marked out on an electronic floor plan by an administrator and a BIM tool can perform computational flow analysis based on geometric reasoning [5] to automatically identify the set of affected doors. The key point is that the BIM is capable of calculating and expressing the correspondence between a logical spatial concept - the Restricted HR Zone - and its physical manifestation in terms of extent and door connectivity. More importantly, it can keep this up-to-date so that the security policy can be expressed at a high level of abstraction using a logical concept that does not need to change (i.e. only HR staff can access the Restricted HR Zone). If the physical space changes this can be reflected in the model and the necessary PACS configuration can be automatically 'recompiled'. This leads to a higher level of assurance that the security policy is actually being enforced, thereby assisting organisations in meeting audit and compliance obligations, which are increasingly onerous for security-sensitive facilities. We provide more examples of spatial access policies in Section 2.

The ability to compute and visualise access control policies that have a spatial dimension is a powerful capability that becomes possible with our proposed BIM-enabled authorisation framework. As we have noted, it allows the BIM to function as a visual design tool to accurately formulate and review access control rules and policies. Since a BIM supports geometrical reasoning [5], with our framework it is possible to calculate and display the areas that will be accessible for a given low-level PACS rule set. New rule sets can also be automatically compiled to the low-level format used by the PACS. Configuration and analysis based on geometric reasoning has the advantage that it can identify indirect access paths that may be overlooked when the configuration is developed or audited manually based on a floor plan e.g., a restricted area may be unintentionally accessible through a complex route via a lower floor. It can also assist a security administrator who wishes to know if a highly sensitive area is indirectly accessible from a lower security area via false ceilings, ventilation ducts or walls made from materials that can be easily breached (as shown in Figure 1).

This is a useful capability when a building is first being designed and subsequently for the facility managers to plan remodelling and partitioning of spaces subject to different access rules. Further, the BIM can also function as an access control simulator that can be used to analyse different access control scenarios such as path finding for evacuation in response to fire in different parts of the building - a capability that could be valuable in developing emergency response plans [6, 7].

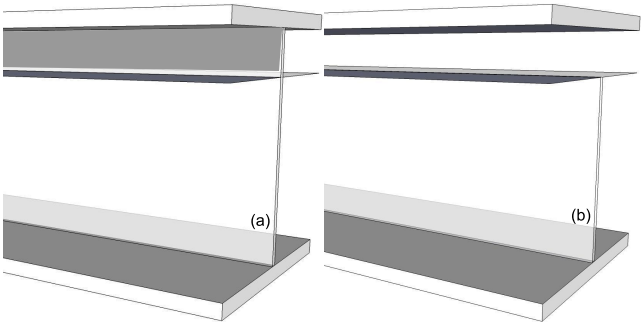

FIGURE 1. The need for 3D models in Security Analysis (a) a wall going up to the underside of the slab of the floor above (b) a wall going up to ceiling height, with the possibility of access through the ceiling space.

The use of spatial attributes in authorisation policies has gained popularity among researchers in the past decade with the widespread adoption of geographic information systems (GIS) and the ability to track resources spatially. However, limited research has been carried out in the area of spatial authorisation for BIMs, which differ from the traditional GIS context, particularly in terms of scale, how three dimensional data is structured and the granularity of spatial information for indoor models. Indeed, to the best of our knowledge, there is no published research on using Building Information Models for access control.

1.3. Converged physical and logical access control

The concept of security convergence [8] merges the physical security and logical security operations to fill in the gaps and interfaces between these two functions and provides more efficient and effective security. An integrated authorisation system for physical security and logical security will enable using two-way interaction between these two systems in decision-making. For example, the logical access control function can infer location status of a user from the physical access control system to determine if the user has entered the specified spatial zone before accessing a spatially bounded information system. Information from a workflow and scheduling system might be used to configure physical access control rules based on task location and required access zones. This approach can enhance security management and access policy definition.

The concept of convergence in access control for physical and logical security systems is based on a unified repository of user identity data and associated attributes [9]. Information technology has permeated physical security systems in recent years. This has brought many security issues to physical security systems that were once specific to

information systems. Even though physical security and information security are managed independently in most organisations, they share the same goal of securing organisational resources. This two-level approach leads to administration overhead and reduces overall control in security [10]. A converged access control approach gives organisations more control and consistency over security management. There are many common aspects between controlling access to information systems and physical spaces. The basic subject, object, and access type relations in information systems can be interpreted as a person, physical structure and physical access type relations in physical access control [11]. One of the goals of our proposed authorisation framework is to apply unified approaches for access control in heterogeneous systems with physical and logical access control subsystems.

The remainder of this paper is organised as follows. In Section 2 we present an example scenario that we will use throughout to illustrate different spatial access control issues. Section 3 discusses different aspects of spatial data models and the central concepts of building information models. In Section 4 we categorise the forms of access control needed for building information models and in Section 5 we summarise the key requirements for a BIM authorisation framework. Section 6 identifies key features of access control models that are able to perform spatio-temporal authorisation. Using these features or distinguishing characteristics as a basis for comparison, Section 7 reviews a number of significant spatiotemporal access control models and their ability to address the requirements previously identified. In Section 8 we propose our conceptual model for an authorisation framework using building information models. Finally we conclude in Section 9.

2. EXAMPLE SCENARIO

In this section, we present an example scenario, which serves to illustrate the concepts introduced in later sections. We consider a facility of an organisation that houses multiple divisions. We assume independent subsystems are used for closed-circuit television monitoring, lighting control, temperature sensors, smoke sensors, and physical access control to building spaces.

Suppose Alice is a divisional human resource administrator who authorises access by employees to different spaces in the facility. She is able to approve and revoke access to users within her division to spaces that are used by her division and common areas. Bob is the facility's operations manager responsible for facilities management. He is able to assign both staff and contracted technicians to perform maintenance on different subsystems such as lighting water and sewerage. He needs to grant access to a contracted technician only when there is a current repair or maintenance job. He must ensure that the technicians cannot access sensitive parts of the facility that are not related to their assignment. Charlie is a computer technician handling the server room, Dave is a technician for the temperature sensors, and Eddie is an electrician responsible for the lighting subsystem. They can access the subsystem controllers from the control room, and Bob controls their access privileges to different spaces.

The building areas are divided into zones to which different access policies apply. Multiple divisions use the building control room and a shared server room, but access is tightly restricted. Further, the general office area is divided based on the occupying organisational division such as marketing, human resources, and finance. The control room houses a command and control application with controlling interfaces to all the subsystems. These can be accessed by either the facilities management team or technicians associated with the subsystems. For example, in a normal operating environment Eddie can access the lighting subsystem that controls the lighting of the building, but not the temperature sensors. The command and control system has two-way communication to the subsystems. The incoming data from the subsystems include the status and operational data from different sensors. The outgoing data include commands and instructions to control the subsystems, which can be used to change the operation of different devices. These commands can be issued directly to the devices or to another system that controls the low-level sensors.

Suppose the command and control application is fed with status data from all subsystems, including each temperature sensor. It can then generate a temperature gradient floor map for the whole building using its knowledge of the spatial position and context of each sensor. The building information model will also store the physical position of other elements such as CCTV cameras, lights, smoke sensors, and door controllers. By representing these active elements on a 2D plan or a 3D virtual space an operator can interact with them visually to issue commands or access status data or information feeds. For example, they could click on CCTV camera icon to view the real-time video stream.

Access control in this organisational scenario can be complex. Alice should be able to control who can access the control room. Charlie can view the temperature gradient map of the server room only, but Dave can have access for the whole building. Eddie can access the status of lighting for the whole building. He can select a particular room from the spatial visualisation and issue a shutdown command. However, this can be executed only when Bob assigns him for a maintenance task in that room. The organisational policy also states any technician entering the server room must be authorised by Charlie in addition to Bob. These complex access control scenarios are difficult to accommodate using traditional access control systems. A primary purpose of our work is to provide a framework that supports

these scenarios. We discuss these different approaches in the following sections.

3. SPATIAL DATA MODELS

This section will introduce existing spatial data models that can be used for spatial representation of buildings and facilities. A spatial data model defines how spatial data are stored and represented within spatial databases. It would also define how these data could be analysed and manipulated. Spatial data models can be divided into two broad categories: outdoor models and indoor models. This basic categorisation stems from granularity, type, and structure of spatial data required for the applications of indoor models versus those of outdoor models [12, 13]. The rest of this section will introduce City Geographic Markup Language, Building Information Modelling, and Industry Foundation Classes, and discuss their features and shortcomings in the context of access control.

3.1. City Geographic Markup Language

Virtual three-dimensional models of cities can be utilised across multiple application domains such as urban planning, disaster management, facility management, and environmental simulations. Until recently, most of these models were used for graphical or geometric representation of environments without the semantic or topological aspects, which are necessary for spatial analysis and data mining [14]. The Open Geospatial Consortium (OGC) developed Geography Markup Language (GML) [15] as a standard for storage and transport of geographic information and as a comprehensive modelling language for geographic systems.[1]

City Geography Markup Language (CityGML) [16] is an XML based storage and exchange format for virtual city models. Technically, CityGML is an application schema of the Geography Markup Language 3 (GML3) [16]. It provides appearance, topological, semantic and geometrical models by defining the classes and relations for the representation of most three-dimensional urban objects such as built structures, elevation, vegetations, water bodies, etc. In CityGML, the appearance model provides "observable properties" for object surfaces, which can be used to represent visual data and other arbitrary categories such as infrared radiation, noise pollution, or structural stress. The CityGML thematic model contains class definitions for important object types that are required by different application areas. Real-world entities correspond to features such as buildings, walls, or doors in the semantic level. At thematic level, extension modules are defined for different application areas such as transportation, vegetation, or waterbody. The thematic classes can contain both spatial and non-spatial attributes. Non-spatial attributes are properties such as creation dates, image URIs, or year of construction. It can also define interrelationships like aggregations, generalisations, and associations for feature classes.

CityGML supports multiple level of granularity through different Levels of Detail (LOD). This provides five independent LODs, LOD0 to LOD4, and each object in CityGML can be represented in different levels of resolution. LOD0 has the lowest class of accuracy that is used to model regions and landscapes. In its basic level, it can represent an aerial image or a map in a two and a half dimensional digital terrain model. Buildings in this level are represented by either footprint or roof edge polygons. LOD1 is a blocks model in which building structures are aggregated into simple blocks with no further details. LOD2 has detailed roof structures and boundary surfaces. LOD3 provides granular details of roofs and walls including doors and windows. It can represent external architectural models and land marks. The levels up to LOD3 in CityGML can be used to model outdoor spaces. LOD4 of CityGML attempts to bring indoor and outdoor representations more closely by considering indoor specific object details. LOD4 provides the highest level of details of all LODs and it adds interior structures of building to a LOD3 model. The *Building* module of CityGML enables representing thematic and spatial aspects of building, including indoor building structure. LOD4 can be used to represent constructive elements in architectural models. The interior structure of a building such as rooms, doors, stairs, and furniture can be modelled in LOD4. Interior installations in LOD4 classify objects that are permanently attached to the building structure and cannot be moved. For example, objects such as pipes, wiring, or interior stairs can be represented as interior installations. These objects can be associated with a room or the complete building.

Even though LOD4 provides the foundation for spatial modelling of indoor environments, it still lacks the functionality and the granularity that may be needed for applications such as indoor navigation [17, 18]. IndoorGML is a work in progress towards an indoor spatial modelling based on CityGML. It is particularly focused on providing a framework for the integration of different positioning and localisation technologies that are used to assist in indoor navigation, but cannot be directly modelled using CityGML [19, 20]. IndoorGML seems to be relevant to our work, however the details of the model are yet to be published.[2]

[1] GML is an XML based encoding grammar developed by the OGC as a feature based modelling language that maps the real world geographic information into feature sets. Refer to [15] for more information.

[2] There are recent efforts to standardise IndoorGML under OGC [21]. To this end, the IndoorGML Standard Working Group [21] was formed in January 2012, however no further information about the status of the standard is available. Refer to their website for more details: http://www.opengeospatial.org/projects/groups/indoorgmlswg

3.2. Building information modelling

The overall goal of building information modelling is to provide a common repository of semantically rich three-dimensional information that can be used seamlessly and sequentially by all members of the design and construction team, and ultimately by the owner/operator of a facility throughout the facility's life cycle [22]. BIM technology extends into fully integrated 3D and 4D modelling (adding the time dimension for scheduling or sequencing) of the building design. This process produces the Building Information Model (BIM), which incorporates spatial relationships, geographic information, building geometry, and quantities and properties of building components, including the life-cycle processes of construction and facility operation. The use of building information modelling in this context has gained increasing acceptance around different industries during the past years [23, 24]. Even though other types of data models such as CityGML exist that can be used for buildings, the wider architecture/engineering/construction (AEC) research community, private sector, and governments have adopted building information modelling as the way forward for buildings [25, 26, 27].

A major element of the success of BIM is establishing common software protocols [22, 28]. The Industry Foundation Classes (IFC) is a leading standard for achieving BIM interoperability. IFC is an object-based data model developed by the International Alliance for Interoperability (IAI) to facilitate interoperability of building information models [22]. IFCs are a commonly used format for BIMs in architectural, engineering, and construction (AEC) industries. The IFC data model is used as the interchange file format between different stakeholders of buildings to exchange software independent building information models. For example, a building information model produced by an architect using computer aided design software can be used by the building operator in the facilities management software. The use of IFC standard enables continuous industry-wide sharing of information for the life cycle of the building.

The IFC is an object-based information model for storing and exchanging data about buildings. It defines a spatial hierarchy - a project contains one or more sites, a site contains one or more buildings, a building contains one or more storeys, storeys contain spaces, walls etc. and spaces contain furniture and fittings. Each object in the model has a standard set of properties, but users can add non-standard information using the in-built extension mechanisms. While the above hierarchy is a strict tree structure, systems of objects can be defined that span multiple storeys or buildings, such as a security control system. A single object can be part of many systems if necessary.

The IfcProduct class defines the base for all physical objects within an IFC model. The IfcRelationship class creates relationships between objects. The five basic relationship representations are composition, assignment, connectivity, association, and definition. For example, when a wall is connected to a beam, the wall object of IfcWall class and the beam object of IfcBeam class can be associated by the relationship class IfcRelConnects. The IfcRelDecomposes class represents containment relationships such as IfcBuildingStorey containing IfcSpaces.

The IFC model is supported by the major architectural CAD systems and an increasing number of engineering CAD and analysis systems. Since most buildings last much longer than the computer software that is used to design them, a major benefit of the IFC model is that it supports an ASCII character-based file format that can be archived to remove dependencies on particular software vendors.

While the IFC model supports file-based exchange, this is not convenient for intensive use of IFC-based representations. Model servers are specialised databases that store information so that it can be continuously accessed and modified by multiple users. If a building is modelled in an IFC compatible CAD system, it can then be exported to a model server, where it can be used to support day-to-day operations. If the facilities management and control systems are integrated with the server, the IFC model will be updated every time there is a change in the building. This will ensure that the current data is always available.

3.3. CityGML vs. BIMs

Both CityGML and BIMs are semantic models that are targeted at different scales and scopes of representations [20]. There are three significant differences between CityGML and BIMs with regards to their suitability as a spatial data model for access control.

First, in CityGML, surface observations of topographic features are used to derive three-dimensional objects. In BIMs, a generative modelling approach is used to represent how a three-dimensional object is constructed [29]. BIMs provide details semantic representations of *all* building elements. A unified BIM for a facility would include objects and elements from all domains, such as architectural, engineering, construction, or facility management. More importantly, BIMs include representations of hidden objects such as pipes, wiring in-between walls, ceilings, and floors with a finer granularity. This is an important feature when we are concerned about all aspects of access control. For example, the possibility of capturing data from communication cables, also known as packet sniffing [30], can only be inferred if the critical network cabling information is available in the data model.

Second, CityGML does not provide a specific concept

for the representation of storeys [16]. Storeys however play an important role in access control. The ability to represent multi-storey buildings and objects that share across multiple stories such as lifts and escalators are important in determining access control. Thus, it is vital to have a concrete representation within the model to support this rather than ad-hoc workarounds that are used in CityGML.

Third, BIMs are used from the preliminary stages of building design and evolve throughout its life cycle. This provides the possibility for security and access control design process to be incorporated from the early stages, rather than as an afterthought.

Due to the above differences and advantages, in the rest of this article, we consider BIMs as a spatial data model for the authorisation framework that will be proposed in Section 8.

4. FORMS OF BIM-BASED ACCESS CONTROL

It is essential to clarify the context of spatiotemporal authorisation in real world applications to understand the need for an advanced authorisation framework using building information models. Figure 2 shows information flows between entities in an authorisation framework that uses a BIM. Each information flow, or each arrow point in the diagram, introduces an access control requirement. We group these access control requirements into two major categories: BIM content and external resources. The external resources can be further categorised based on their interaction with BIMs as BIM-aware and BIM-unaware. In this section, we look at some of the operational scenarios of these access control categorisations.

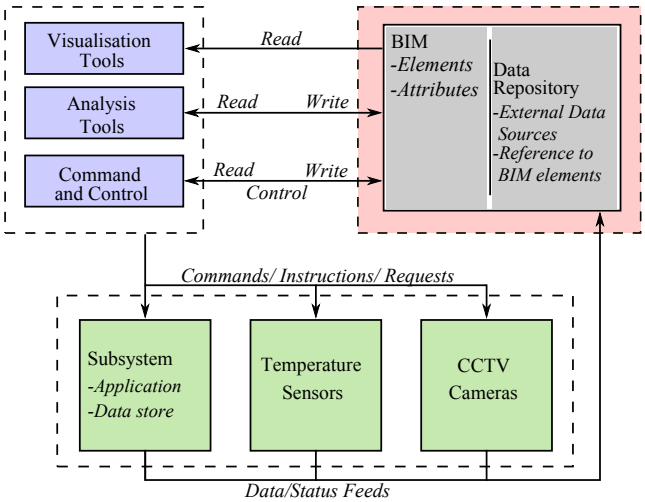

FIGURE 2. Information flow between building information model and subsystems

4.1. Access control for BIM content

In this category, we are focused on controlling access to data contained within a BIM representation - the BIM content. There are two distinct sub-categories of resources requiring controlled access: firstly, the building elements and their associated attributes (i.e. elements that can be represented as IFC objects); secondly, any data or information fed from external sources that is stored in a separate data store, but closely coupled to existing BIM elements via their unique identifiers. This data store can be used to archive data generated by external systems that have no native spatial awareness, to give the data spatial context e.g., temperature readings from sensors linked to the HVAC system can each be stored together with the unique identifier of the BIM object representing that sensor. The data can then be analysed and represented spatially.

There are multiple modes of access required for BIM internal data as shown in Figure 2. For example, a visualisation tool may only require read access to BIM objects to render a floor plan and overlay temperature gradients based on sensor readings from a linked data repository. Systems that can manipulate the BIM and make changes to building elements or internal data will need read and write access. For example, an analysis tool that performs computational analysis on elements of the building and stores results back in the BIM comes under this category. Command and control type systems will use BIMs as a tool and issue control commands to linked subsystems based on spatial relationships of resources and systems. These systems can also issue commands to external systems to bring in information updates, such as sensor data.

The concept of using a building information model as a unified interface and data repository for different subsystems is central to leveraging BIM for facilities management. As we have noted, the spatial context provided by the BIM can make previously independent subsystems easier for users to interact with. For example, a CCTV camera feed could be accessed by clicking on a camera icon on a floor plan. However, not every system or user needs to be given access to every information feed when they have access to the BIM - the security policy may restrict access to data from CCTV camera feeds to on-duty security operators who are present in the control room. Further, the policy may authorise remote CCTV access to emergency response officials but only when the system recognises that an emergency has been declared. Users who hold the role of computer technician can be granted access to view only the CCTV feeds for the server rooms by selecting the relevant rooms on the visual map. The BIM stores information on which individual cameras are in each room and the low level access privileges can be compiled from this spatial context. This same principle can be applied for access control to other types of logical

resources that have a spatial context.

Clearly, the resources and information that can be accessed via a BIM vary in sensitivity and the BIM authorisation system needs to be able to record and enforce complex access rules as our examples have illustrated. Unfortunately, current BIM tools and BIM servers implement only the most basic access control features if any at all. Model development tools from commercial vendors such as Autodesk do implement some role-based access controls but these are focused on the design phase, not a building's operational phases that are the principal concern of our framework.

4.2. Access control for external resources

In this category, we are focused on controlling access to systems and resources that are outside the BIM, but we wish to leverage the spatial information in the BIM to express and enforce the policies (access rules). Thus, access control for external resources includes logical access to information systems and information resources, and physical access to physical objects and locations, all connected within a spatial and logical context via a BIM. This context information is used in access control decision making. As we will discuss shortly, this approach enables the integration of physical access control with logical access control which yields a number of security-related advantages.

Plant, equipment, machines, etc. in a facility are increasingly computerised and managed via process control hardware and software (e.g., Supervisory Control and Data Acquisition or SCADA) over internet-connected networks. They are evolving to have many of the characteristics of traditional software applications. Though their authorisation capabilities are relatively immature [31] some can distinguish different users and grant them specific access privileges. For improved efficiency and security, these disparate systems need to be managed in a unified way.

Computerisation and network-based control makes it possible to access systems remotely. This increases the likelihood that they will be maliciously attacked. For example, a disgruntled ex-employee may be able operate or disable equipment via an internet connection to cause damage or financial loss to the organisation [32]. To combat remote access threats, certain types of access need to be restricted, for example, on the basis of the location of the resource and the user. Even if a user has been granted access privileges to a control system (e.g., HVAC, lighting, waste water) the security policy may stipulate that they need to be physically present in a particular location to execute critical functions. So the maintenance electrician Eddie may be permitted to monitor equipment status remotely, but he must be physically present in the control room to issue shutdown commands. The integration of physical and logical access control and a spatial model can allow this condition to be enforced. The framework can verify if the user has entered the designated space via the physical access control subsystem, before granting access to the information system.

4.3. Access control administration

Creating access control policies is a critical task in any authorisation system. The use of multiple attributes such as spatial, temporal, and other constraints makes access control rules complex to define, maintain and audit. We propose a mechanism that utilises BIM and its spatial model to make this process more intuitive for privilege administrators.

Consider our example in Section 2, where Alice needs to configure access to a new employee joining their division. She has already defined the spaces occupied by her division and, based on geometric reasoning, the system has computed the other zones and doors that must be accessible to reach that space with the least privilege required. These spaces can be referred to in access policies via a logical tag e.g., *Finance Division Zone*. Alice simply needs to assign the new employee the role of Finance Division member and the authorisation framework will utilise the relationships in the BIM to assign the required fine-grained access privileges to the new employee. This can be done automatically via a rule that says finance staff can access the finance zone. Our approach to spatial policy creation, visualisation and enforcement gives greater assurance that high-level security policies are correctly implemented.

Dynamic generation of access control privileges is a desired feature of an authorisation framework. For example, Bob can assign Eddie for repairs to different parts of the building each day via individual jobs generated through an asset management system linked to the BIM. The location of the effected equipment and the status of the jobs can be used to automatically assign and revoke physical access privileges in the PACS.

Access control policy visualisation provides a visual representation of authorisation policies. The system operators will be able to visualise the access possibilities for a user or a group of users using the spatial model. For example, fine-grained physical access control rules, which determine whether a user is able to open a particular door, can be geometrically analysed and displayed graphically on a floor plan of the building to visualise the areas of the facility that are accessible to a particular employee.

The ability to visualise access control policies is essential for simulating emergencies and evacuation plans [33, 34]. Access control patterns change during an evacuation event and physical access control to doors and control spaces are reconfigured to enable emergency response and recovery. The ability to test policies for these different scenarios is useful in eliminating unwanted access situations. This can be used in

conjunction with an emergency response subsystem and assist emergency response teams in planning.

5. FUNCTIONAL REQUIREMENTS FOR A BIM-BASED AUTHORISATION FRAMEWORK

In this section, we introduce the key requirements for an authorisation framework using building information models.

Spatial data model: The main aspect of an authorisation framework using building information models would be the ability of using it as a spatial data model. It is required to provide the vocabulary for naming these entities of different types in a spatial context in access control policies and for decision-making functions. The data model should also include semantics for operations on these objects, including spatial operations that can complement the core decision-making process.

Objects: An authorisation framework for buildings must enforce access control for physical spaces, physical objects, and logical objects. These resources could have a variety of groupings based on feature type, object content, metadata, and spatial position. In addition, the same authorisation mechanisms should be able to access control data contained with building information models. The authorisation framework could utilise the same policies and decision-making processes as it relies on the same data model to provide the vocabulary.

Subjects: Access control enforcement should take into consideration the organisational functions performed by users. The system should have the capability to specify rules based on conceptual groupings of users that are based on their organisational functions or roles. In such an authorisation framework used in large facilities it is desirable to have role based access control (RBAC) [35] capabilities. Subjects should also have additional attributes, such as current location for human users and these locations can point back to an entity in the spatial data model.

Policy: A range of different contextual factors should be specified in the authorisation policies for operations that can be executed on the controlled resources. Attributes such as user location, time of request, resource type, resource location, and access mode could be used in specifying rules for access control. The main vocabulary of the policies will be derived from objects of the spatial data model.

Authorisation policies that define the access privileges should be activated or deactivated by event triggers to handle emergency scenarios and event response. These policies should dynamically change the accessibility of protected resources in such events. However, basic security and privacy requirements should be enforced at all times. Policies must be auditable to ensure no errors or inconsistencies are present that can lead to unintended access or violation of constraints. Any disclosure of additional data or any provision of additional access must be made on a need-to-know basis. To ensure that the authorisation system can be managed efficiently, roles, resources and spaces should be arranged in hierarchies so that policies can specify constraints at varying granularities.

Decision-making: The policy-reasoning component of an authorisation framework is a decision-making point for access requests. Access control decisions made by the framework should be based on multiple attributes of the subject, object, action, and the environment. Access privileges assigned to a user and the function to enable and disable them must be based on a combined spatial and temporal approach delivering dynamic spatiotemporal permission assignment. This may also include awareness of the state of execution of a structured workflow or business process.

Spatial awareness: The decision making point should be able to interpret user location and resource location from the spatial data model, and it must be able to utilise spatial functions that operate on these objects in the decision making process. The spatial data model and an associated spatial reasoning component should provide spatial functions such as containment, connectivity, and accessibility that operate on objects contained within the spatial data model.

Interoperability: The authorisation framework should be interoperable with multiple subsystems. It should be possible to integrate geospatial data from heterogeneous sources in a secure fashion. The access control features enforced by this framework should complement any existing security mechanisms of the subsystems. The authorisation framework should act as an additional layer on top of these systems that can run on different technologies. The individual subsystems can implement their own security policies to protect their data. Thus, policy interoperability is an important consideration in achieving interoperability between multiple subsystems. Attributes and targets of the policies should be interpreted consistently and any mismatch of policy rule semantics and rules avoided.

Integrity: Integrity of data should be ensured, when it is resourced from and managed by third party entities. This is essential when different subsystems are integrated. Privacy is also a greater concern in data flow among multiple subsystems. It should be able to control and enforce access rules across existing physical access control system from different vendors. The spatial location coordinates should be independent of the devices used to capture them. The use of logical

representations for physical locations or zones should be supported to present a unified location representation, which is essential for interoperability between multiple subsystems. The visualisation of the spatial data should take into consideration the possibilities of inference when the absence of certain elements could imply the existence of something sensitive.

6. FEATURES OF SPATIOTEMPORAL ACCESS CONTROL MODELS

In this section, we describe and discuss features relevant to access control models in the context of spatiotemporal authorisations and building information models. Similar to [36], we identify and discuss features in terms of uniqueness, relevance, shortcomings, and other issues. We summarise the key features of these access control models in Table 1. These features form the basis for of our analysis of noteworthy spatiotemporal access control models will be discussed in detail in Section 7. The following sections describe key features that we have used for a conceptual comparison of spatiotemporal access control models.

6.1. Formal foundation

The role of access control systems is to enforce an organisation's security policies. The security-sensitive nature of access control often motivates authors to present a mathematically precise description of their model to support claims about its capabilities. The formal presentation of a model defines its entities and operations and a range of underlying descriptive formalisms can be found in the literature, with set theory being a popular choice. The formalism used to describe a model does not need to be the same as that used in actual decision making. For example, GSTRBAC [41] uses set theory to define the model and predicate logic to define access policies and implement authorisation decision making.

6.2. Support for role-based access control

It is desirable to use role based access control [44] for spatial authorisation frameworks when they are used in large organisations. In such systems, permissions can be associated with roles based on organisational functions performed by users. By centralising the administration of permissions for large number of users this can effectively reduce errors and redundancy. Many of the spatiotemporal access control models use the conceptual foundation of RBAC to achieve these requirements. The notion of role in RBAC is extended to spatial role, temporal role and spatiotemporal role in some of these models. They also use the concepts of role activation and deactivation, role hierarchy and other role based relationships. It has been argued that RBAC has a number of advantages over other models of access control, particularly in simplifying authorisation administration [35]. Here we discuss RBAC as a feature for spatiotemporal access control models.

Four modular variations of RBAC can be identified based on their functional capabilities [44]. RBAC0 represents essential RBAC capabilities including roles, user-role assignments, and permission-role assignments. In large organisational settings, RBAC roles can have capabilities that are overlapping where users of different roles with common permissions. It would be inefficient to have these permissions for each role assignments and many RBAC models implement the concept of role hierarchies. RBAC1 adds the support for role hierarchies to flat RBAC0 as a partial order relationship between roles [45]. RBAC1 defines a seniority relationship between roles through hierarchies and permissions are inherited among roles.

Separation of Duty (SoD) is considered a fundamental principle in computer security that guarantees major errors do not occur without intentional consent of multiple users [46]. Users of different functions are assigned to specific tasks to minimise collusions. RBAC2 enables separation of duty relations for RBAC [47]. RBAC2 supports both static and dynamic SoD. Role constraints are evaluated against user role assignments in static SoD, whereas in dynamic SoD it is against the set of roles activated for the user in the active session.

The fully featured RBAC model, incorporating RBAC0, RBAC1, and RBAC2 is identified as RBAC3. Many of the spatiotemporal access control models use the conceptual foundation of RBAC in one of the variations. The notion of role in RBAC is extended to spatial role, temporal role and spatiotemporal role in some of these models. They also use the concepts of role activation and deactivation, role hierarchy and other role based relationships.

Even though RBAC has many advantages, it can be challenging to apply in many real world settings. A notable criticism is that it is difficult to setup an initial role hierarchy and assign coherent and correct sets of privileges to individual roles [48]. In addition, roles need to be under a single administrative domain or have a consistent definition across multiple domains for proper operation of RBAC. Thus using RBAC with distributed applications is challenging. Furthermore, many real-world applications, including the BIM-based scenarios we have described, require access restrictions imposed not only based on roles, but also considering other dynamic, context-dependent criteria. With traditional RBAC, access decisions do not consider factors such as user location, resource location or system time, which may be as important as roles for access decision-making in some settings. A number of proposals have been published that aim to address this issue by making RBAC more context-aware through the addition of context attributes to decision making [48]. These models are discussed in the following sections.

Features	GRBAC (2000)[37]	GSAM (2004)[38]	GEO-RBAC (2005)[39]	STRBAC (2007)[40]	GSTRBAC (2007)[41]	ESTARBAC (2009)[42]	GeoXACML (2008)[43]
Formal foundation	Not formalised	Set theory	Set theory	Set theory	Set theory and predicate logic	Set theory	Defeasible Description Logics theory
Role-based access control support	RBAC3	No RBAC. Geospatial and credential type hierarchies	RBAC3	RBAC3	RBAC3	RBAC0	XACML RBAC Profile
Spatial data model	None	Vector maps and digital raster images	A reference geometric model	Three-dimensional geometric space	None	None	OGC Simple Feature Access Geometry Class Model
Spatial granularity	Unspecified	Multiple resolutions of images	Point, line, polygon object types and collections	Physical points, physical locations, logical locations	Unspecified	Physical point and spatial extent	Multiple geometric classes
Temporal constraints	Yes	Limited	No	Yes	Yes	Yes	Possible
Policy specification	None	Sets	Unspecified	Sets	Alloy	XML	GeoXACML Policy Language
Policy administration	No	No	Yes, in later proposals	No	No	No	Yes
Multiple policy integration	No	No	No	No	No	No	Yes
Physical access control	Possible	No	Possible	Possible	Yes	Possible	Possible
Logical access control	Possible	Yes	Yes	Yes	Yes	Yes	Possible

TABLE 1. Summary of Access Control Model Features

6.3. Spatial data model

Spatial access control is based on the spatial context of resources and requesters. A data model is required to provide spatial context to all entities concerned with the authorisation system. Access control policies will be defined using spatial specifications of the spatial data model. Authorisation decision-making procedure will use the spatial data model to make access control decisions based on access policies.

Spatial data models used in access control models can be based on basic geometrical coordinates as in STRBAC, or vector based reference models such as in GSAM. A majority of the existing spatial access control models use three point coordinate systems as the spatial base. The combination of vector maps with digital raster images is commonly used in many geospatial applications. It is desirable to have a flexible data model such as a building information model that can streamline spatial data management. It is also desirable for this data model to be standards compliant to achieve interoperability between different systems associated with the authorisation system.

For instance, when analysing access between rooms, the thickness of walls is not a major concern. The concern is about openings in walls (ie doors and windows) and access control through these openings. For security analysis purposes, we normally only need the rooms (spaces) themselves and the boundaries between them (Figure 3). These spatial association information from the spatial data model can be used in the access control process.

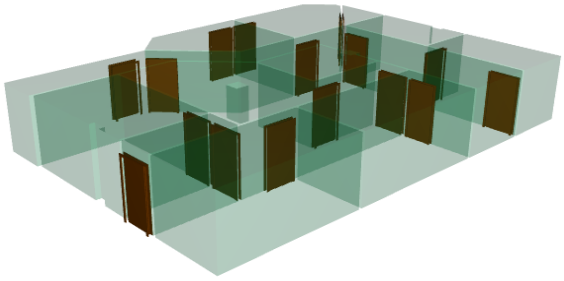

FIGURE 3. Multiple Space Boundaries

6.4. Spatial granularity

Authorisation systems are required to provide access control at different levels or granularity. Many real world entities can be mapped spatially at different levels such as a town, block, building, floor, room, and even individual elements. Based on the level of control required the access control system needs to address protected elements at varying levels of spatial granularity.

A spatial hierarchy of protected objects simplifies the policy definition process, where permissions assigned to higher-level objects can be derived at lower levels. For example, a geospatial system using raster image maps for its spatial representation can generate maps at different resolutions and with different sets of object overlays based on the access control decision. Some access control systems simply rely on geometric coordinates and others use multi-level logical locations. The concept of logical locations maps a real world spatial entity through a mapping function to an entity in the selected data model. This can provide flexibility

in defining and processing access control policies. For example, a controlled door to a secure server room can be represented by its three-dimensional coordinates *(x,y,z)*. This can be mapped to a physical location using a mapping function m that converts the coordinates to a logical representation of type *room*, and subtype *secure area*. The inverse mapping function m' can be used to convert logical locations into physical coordinates.

The degree of spatial granularity can have both a positive and negative influence on the efficiency of decision making and the expressiveness authorisation policies. A finer level of granularity ensures that it is possible to express a wide range of access rules and associated constraints. This can also lead to increased searching and processing time for access control policies and decision-making, which can negatively influence the real-time performance of the authorisation system.

6.5. Temporal constraints

Many organisational functions can have limited or periodic temporal duration and resources have temporal limitation on availability. Therefore, access control to resources needs to have a temporal dimension in decision-making. The need for expressing authorisation rules on the basis of temporal relationships in real-life situations has been recognised by other researchers [49, 50, 51]. Temporal dependencies allow the derivation of new authorisations based on the presence or absence of other authorisations in given time intervals [50]. Authorisation rules can specify a start and an expiration time. Both negative and positive authorisations can be specified explicitly or derived through rules [52]. Periodic temporal intervals are used to grant and revoke authorisations automatically [53].

6.6. Policy specification

Policy specification concerns how policies are expressed. The common policy specification approaches for spatiotemporal access control systems include sets, logic-based languages, graph theory and combinations of these. Access control models such as GSAM and STRBAC, which are defined using set theory, rely on sets for policy specification. XML based mark-up languages can be used in access control frameworks for policy specification. XACML and GeoXACML use logic-based authorisation languages for policy specification. These logic-based languages can improve the process of verification, modification, and enforcement of policies, because of their formal foundations and expressiveness [54].

6.7. Policy administration

Policy administration is the task of creating and maintaining access control policies by security administrators. In large organisational environment, a proper administration mechanism of complex access control policies is a critical aspect of any authorisation system. It is required to ensure the specific intentions of security administrators are rightly reflected in the access policies. Such large organisations can have thousands of users, roles, and resources and their access control policies can define large number of complex and fine-grained rights that are managed by different administrators [55]. In addition to these complexities, spatial authorisation systems have another dimension of spatial roles, resources and rights, which makes policy administration even complex [56]. Thus, policy administration is an important feature to consider in reviewing spatiotemporal access control model. The task of constructing and maintaining such complex access control policies is non-trivial and proper tools and mechanisms are needed. Most of the spatiotemporal access control models we have reviewed do not incorporate policy administration in their initial proposals. However, this need is commonly identified later and some models have later extensions that provide policy administration [57].

6.8. Multiple policy integration

It is necessary to achieve integration of access control policies when multiple organisational divisions are combined under one authorisation domain or multiple subsystems are integrated into a larger system. This integration process must combine independently defined policies from different divisions, while ensuring independence and administrative autonomy [54]. Policies from different authorities must be integrated and enforced without ambiguity in an enterprise-wide authorisation framework. This means that the policy language must support a range of strategies for resolving conflicts between the decisions generated by different individual policies since one may permit while another denies.

The process of policy integration is influenced by the policy specification mechanism of each subsystem. It is desirable to have a uniform policy specification standard across all systems, but this is not practical as it is largely dependent on vendor technology and the need to accommodate legacy systems. Logic based policy specification can support policy integration using operators such as addition, conjunction, negation, closure, scoping restriction, overriding, and template [58]. For example, the conjunction operator merges and returns the intersection of two policies.

6.9. Physical access control

Physical access control regulates access to physical spaces within a facility. It can be enforced by controlling individual portals such as doors leading to the specified space. As we have argued in Section 1.3, there are benefits in a converged approach to access control where the same authorisation framework can be applied across logical resources and physical resources.

However, the existing spatial access control models are not designed to handle this scenario directly in their implementations. In some cases, where they do not distinguish between logical and physical resources it is possible to simulate and extend the models to support physical access control. In general, this is a feature lacking in authorisation systems, including spatiotemporal systems.

6.10. Logical access control

Logical access control regulates access to information objects and information services provided through computerised information systems. In spatial authorisation, logical resources include the elements of a building information model, spatial maps, data, and information sourced from other connected systems with spatial context such as CCTV camera feeds. Logical access control is the main focus of the existing spatiotemporal access control models. While some of these systems focus on protecting spatial information contained within maps, others focus on protecting all types of data with spatial context.

7. REVIEW OF SPATIOTEMPORAL ACCESS CONTROL MODELS

In this section, we review a collection of spatial access control models against the model features identified in Section 6 and the requirements identified in Section 5. We cover six systems in some detail: GRBAC, GSAM, GEO-RBAC, STRBAC, GSTRBAC, and ESTARBAC. We focus on these models because they represent a variety of approaches to spatial authorisation. We also include the GeoXACML standard to this discussion, which has capabilities for declaration and enforcement of geo-specific access restrictions. We are interested in its policy framework and capability of integrating access control policies from multiple stakeholder systems.

7.1. GRBAC

Generalised role-based access control (GRBAC) is an early role-based access control model that introduced the concept of environment roles as distinct from subject roles [37]. Any system state that can be collected by the system can be an environment role in GRBAC. An environment role can be based on temporal context such as time of day or day of the week, or location context such as ground floor of the building or third room on the first floor. The environment roles in GRBAC and the subject roles in RBAC have similar properties including role activation, role hierarchy, and separation of duty. These roles can be activated based on the current environment context.

GRBAC can be seen as one of the initial spatiotemporal access control models. It covers the access control problem as for logical or physical resources. These concepts can be extended to both physical and logical access control to achieve a converged approach. GRBAC lacks a spatial data model, and serves only as a higher-level model for spatiotemporal authorisation. The model specification is very abstract with no formal foundation. It does not provide any specifics on authorisation rule definition, or spatiotemporal constraints for environment roles. GRBAC does not address many of the higher-level requirements such as event triggers, granular rule specification, or policy interoperability between multiple systems. Some of these shortcomings of GRBAC were addressed by later models that we discuss in this section.

7.2. GSAM

The Geo-Spatial Data Authorisation Model (GSAM) proposed by Atluri and Chun is another pioneering work in considering the combined impact of location and time in authorisation decision making [38]. GSAM provides protection mechanisms that address issues specific to spatial imagery data stored in spatial databases i.e., Geographic Information Systems (GIS).

GSAM evaluates requests to display or manipulate spatial data and makes authorisation decisions which may involve rendering maps at different detail levels based on criteria such as authorised subjects, objects, and spatiotemporal constraints. GSAM supports privilege modes specific to geospatial data (e.g., zoom-in, overlay, identify, animate and fly-by) and includes geometric considerations such as the region of overlap in access requests and authorisation. It supports geospatial and credential type hierarchies that can be used to specify authorisations and individual identities or geospatial objects can inherit permissions and obligations. GSAM makes authorisation decisions based on spatial extent, temporal duration, map image resolution and other spatiotemporal attributes.

GSAM does not provide mechanisms to extend the authorisation mechanism to other object types such as physical objects or logical system resources. Thus, in the form described, it cannot be directly used in conjunction with other physical or logical access control systems, though its general concepts may be adapted. The temporal aspect of authorisation in GSAM is limited to the temporal terms attached to the map data. It does not use the temporal conditions of the access requests in decision-making. The limitations in role-based access control and specifying organisational roles without geographical constraints limit the use of GSAM in many environments. The lack of standards in authorisation specification can cause interoperability issues with multiple systems and supporting other features like policy migration and cross verification.

7.3. GEO-RBAC

Bertino et al. proposed the GEO-RBAC model[39], extending RBAC with a spatial model compliant with

the OGC (Open GeoSpatial Consortium) simple feature geometric model [59]. GEO-RBAC is formally defined using the principles of set theory and uses contextual information such as user position with the concept of spatial role to make access control decisions.

GEO-RBAC is based on a reference geometric model, spatially aware objects, spatial roles, and a position model. The reference geometric model is based on the OGC simple feature geometric model. An object can be composed by one or more point, line, or polygon types and different topological relations can be applied to the objects in the reference model. This gives the ability of specifying objects at different granularities.

The position model assigns users logical positions that are device/technology independent, based on their real positions using specific mapping functions. For example, a real-time location device carried by an employee can transmit their location as three-dimensional coordinates, which can be mapped to a specific room, which is identified by its logical label in the position model. The granularity of these logical positions can depend on the spatial role played by the user.

A spatial role in GEO-RBAC represents a geographically bounded organisational function, with a role name and spatial boundaries defined by a spatial extent. For uniformity, this model considers non-spatial roles as a subset of spatial roles having the full reference space as role extent. The basic access control concepts of GEO-RBAC for logical resources can be extended to physical access control. Prox-RBAC, an extension of GEO-RBAC, introduces proximity constrains into spatial authorisation syntax with continuity of usage [60]. This is particularly relevant to buildings as the concepts proposed in Prox-RBAC are more specific for an indoor space model.

GEO-RBAC supports role schema and role instance hierarchies that enable inheritance of permissions, user assignments, and activations between roles. It also uses constrained RBAC that extends standard separation of duty constraints for specific characteristics of GEO-RBAC, such as different granularity and spatial dimension [61].

Temporal access control is a vital requirement in many applications but GEO-RBAC lacks a temporal capability. This limitation is addressed by later spatiotemporal access control models. GEO-RBAC does not use any policy specification standard, which could make interoperability difficult. Policy administration is also not part of GEO-RBAC but later proposals address this issue by extending with GEO-RBAC Admin [56, 57, 62]. GEO-RBAC also lacks some of the important requirements, such as multiple object attributes, and policy integration.

7.4. STRBAC

Ray and Toahchoodee formalised a spatiotemporal RBAC model, called STRBAC [40] that considers the interaction of location and time contexts with the classical RBAC components in access control decision-making. STRBAC is formally defined using set theory. Access control permissions are expressed via multiple set relations.

STRBAC does not provide any formal definition of a spatial model, but it is assumed that controlled objects will have devices that transmit location information. It uses the physical location and logical location concept, where physical locations are real-world three dimensional coordinates, and logical locations are their symbolic representations, such as rooms and floors. Mapping functions are used to convert between the location representations. STRBAC uses two temporal information types: a discrete point in time is represented by a time instant and a set of time instances are grouped into a time interval. This enables the use of different semantics in defining temporal constraints.

Spatiotemporal permissions in STRBAC can be associated with roles, objects, and operations. Spatiotemporal constraints can be expressed on role activation, role hierarchy, separation of duty, user-role assignment and role-permission assignment. STRBAC supports multiple role hierarchies for permission inheritance and role activation. Each of these can be unrestricted, time restricted, location restricted, and time-location restricted. STRBAC can control access to physical and logical objects. It assumes every logical object is contained within a physical object, such as a computer. Access control to physical spaces can also be achieved by making an access door the controlled physical object. STRBAC uses sessions to enable pervasive computing requirements. In this mode of operation, sessions are associated with locations and time durations in which roles can be activated [63].

STRBAC does not define any specific spatial data model, making the model specification more abstract without any details for location representations. This model is proposed for computing environments with a single administrative authority. Thus it does not address the possibility of multiple authorisation domains or policy integration requirements.

7.5. GSTRBAC

GSTRBAC is a formal framework for specification and verification of spatiotemporal role-based access control proposed by Samuel, Ghafoor and Bertino [41]. It incorporates topological spatial constraints to the existing GTRBAC model [64]. Both logical and physical access control are possible in GSTRBAC.

GSTRBAC is formally defined using set theory and predicate logic. The spatiotemporal authorisation functions in GSTRBAC use logic operations for decision making. GSTRBAC uses a lightweight formal mod-

elling language, Alloy, for its policy specification framework. This includes policy composition, visualisation, and conflict resolution processes. It enables the policy administrator to validate policies before implementation.

GSTRBAC uses spatial constraints in role enabling, user-role assignment, role-permission assignment, and role activation. The spatial constraints are based on physical locations and virtual locations, but the model does not specify any spatial data model for these locations. It evaluates constraint expressions in the temporal domain to make access control decisions. However, the permissions do not have a spatiotemporal context. GSTRBAC introduces the concept of spatial separation of duty constraints, preventing a user from activating multiple roles simultaneously based on where the role is activated. The spatial role hierarchy enables permission inheritance based on the role activation location.

7.6. ESTARBAC

The Spatiotemporal Role Based Access Control (STARBAC) [65] model proposed by Aich, Sural and Majumdar covers the fundamental requirements for access control with conditions in both space and time domains. It is based on propositional logic and uses logical operations on various spatiotemporal commands for access control evaluation. The Enhanced STARBAC (ESTARBAC) [42] extends the capabilities of the STARBAC model. It includes the concept of spatial separation of duty and algorithms for access control evaluation, which are not part of STARBAC.

ESTARBAC is formally defined using set theory and set operations. Spatiotemporal evaluation functions are also used in access control decision making. ESTARBAC does not use any standard spatial data model. It supports different granularities of spatiotemporal attributes. A physical point is the fundamental spatial unit and a collection of physical points is defined as a logical location. A time instant is the fundamental time unit and periodic expressions are used to specify temporal authorisation rules.

In ESTARBAC subjects, objects, and permissions can be associated with a spatiotemporal extent. An entity in the spatiotemporal domain confined in a spatiotemporal zone is referred to as a spatiotemporal extent. Access control policies in ESTARBAC are defined using role extent and permission extent constraints. A role extent combines organisational role with spatiotemporal extent and a permission extent combines organisational capability with spatiotemporal extent. A user can activate a role and can execute any permission available to the role only when the role extent and permission extent satisfy the user's spatiotemporal extent.

ESTARBAC uses XML for policy specification and uses a policy loader for loading and processing policies into the system. This standardised approach for policy specification allows the model to implement some important requirements, such as interoperability, multiple policy integration, and policy integrity evaluation. However, as proposed, ESTARBAC is intended for use under a single policy administrative point, and integration of policies from multiple entities is not part of the model specification. The access-controlled objects are limited to logical objects with spatiotemporal context. It is possible to extend this model to support access control for physical objects and physical spaces.

7.7. GeoXACML

Geospatial eXtensible Access Control Markup Language (GeoXACML) defines a geospatial extension to the XACML standard by OASIS. Matheus [66] presented an approach for the declaration of spatial, class-based, and object-based access restrictions using the XACML standard specifically for geospatial applications. This was later standardised by the Open Geospatial Consortium (OGC) as the Geospatial eXtensible Access Control Markup Language Encoding Standard (GeoXACML) [43]. Spatial data types and spatial authorisation decision functions based on the OGC Simple Features and GML standards are incorporated into XACML with this extension.

The spatial model of GeoXACML is based on the OGC simple Feature Access Geometry Class Model. This enables interoperability with the OpenGIS web services standard. GeoXACML defines uniform resource names according to the XACML extension points to incorporate geometric attribute values. Multiple levels of GML geometry types are used for the geometric attribute values[67], including Point, LineString, Polygon, MultiPoint, MultiLineString, and MultiPolygon.

GeoXACML policy language can be used to declare complex spatial restrictions with rule constructs. Complex constraints between permission geometry and the resource object's geometries can be expressed through spatial conditions. The GeoXACML specification does not provide any formalisation of the standard. However, it should be possible to apply the Defeasible Description Logics based formalisation of XACML[68] to GeoXACML, as both standards follow the same authorisation principles. An authorisation decision in GeoXACML is made by traversing policy trees and using rule-combining algorithms. Logic operators are used to combine the outcome of subroutine rule constructs into single access decision. Integration of policies from external namespaces is an integral part of XACML and the same is available in GeoXACML.

GeoXACML is different from the other access control models discussed before. It is essentially a policy language and implementation framework. It can be configured to support different modes of

spatiotemporal access control to both physical and logical resources. GeoXACML also supports the XACML RBAC Profile [69] extension that supports the notion of roles for RBAC models that includes support for hierarchical and constrained RBAC. XACML also has a published specification for policy administration and delegation. There is also a GeoXACML specific layered administration model for distributed administration of complex spatial access control policies [55].

7.8. Summary of review

We have analysed some of the important spatiotemporal authorisation models in this section. Each of these models has different strengths and weaknesses as shown in Table 1, allowing them to satisfy different sets of requirements. We have identified the important shortcomings of these models particularly in relation to an authorisation framework using building information models.

A building information model can provide granular information about the relationships between controlled building elements. The notion of adjacent spaces and flow analysis of controlled spaces can be performed by utilising building information models. Most of the access control models we have discussed do not use any spatial data model that has as rich an information set as a building information model. GSAM is a notable exception that uses a richer spatial data model, which is a combination of vector data maps and raster image maps. These vector data maps are conceptually similar to building information models, but on a larger scale with lesser details of individual buildings. The use of logical object hierarchies with physical spatial attributes is the common approach in most of these systems. Even though some of these processes can be performed using basic spatial functions, the use of building information models can give more native approach to the problem.

Policy specification is another important element in access control. It is necessary to have a formalised policy specification mechanism to integrate systems from different vendors under the same authorisation framework. GSTRBAC and ESTARBAC use standardised approaches to policy specification, but they do not elaborate on policy integration issues. The GeoXACML policy framework encapsulates the requirements of policy integration. With the exception of GeoXACML, none of the existing spatiotemporal access control models addresses the need for policy integration, in terms of multi-level policy specification or multivendor subsystems.

Spatial visualisation and evaluation of access control policies can improve the reliability and integrity of the access control framework. A well-structured spatial model is necessary to achieve these requirements. It is possible to implement some of these requirements on top of some of these models. However, the authorisation framework and spatial model must be closely coupled to use two-way information sharing, which can deliver advantages at multiple levels. Most of these access control models do not provide converged access control natively. They are designed either for logical access control or for physical access control.

In the next section, we propose an authorisation framework incorporating a building information model to address the main issues identified.

8. AUTHORISATION USING BIMS

In this section, we present our conceptual model for an integrated authorisation framework, shown in Figure 4. This functions as an overarching access control system for BIM elements, internal resources, and external resources. This authorisation framework will utilise building information models in three key stages of access control: policy design, policy management, and decision-making. Each of these processes use different set of components of the authorisation framework along with BIMs to achieve desired results. The following subsection provides a brief description of each component and later we discuss how each of them interact in each process.

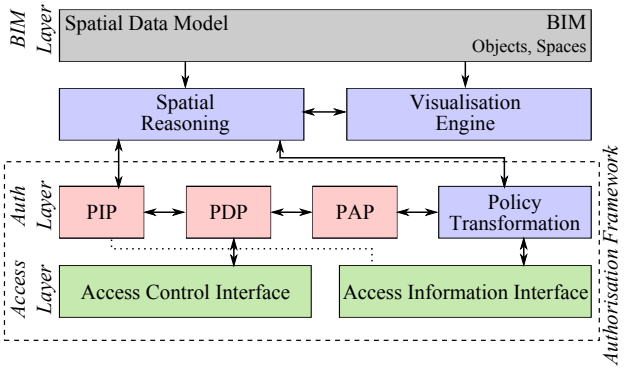

FIGURE 4. Conceptual model of the proposed authorisation framework

8.1. External modules

The authorisation framework will rely on the following external modules for spatial and BIM related operations and these modules must be implemented to an acceptable industry standard.

8.1.1. BIM / Model Server:
The BIM layer consists of BIMs that are loaded into a model server. The BIM files originate from multiple stakeholders of the facility that are converged into one BIM in the model server. The BIMs in the model server are continuously updated with any changes and modifications to the building. The model server can always provide current version of BIM to external systems including the authorisation framework.

8.1.2. Spatial Reasoning:
The spatial reasoning module provides the spatial reasoning functions required for authorisation framework. The BIM analysis tool analyses BIM data and provides computational results at different points of the authorisation procedure. This includes different spatial functions such as locating access doors to a space, reachability analysis based a specified starting and ending points, or obtaining the list of temperature sensors contained within a given space. Referring back to our example scenario, spatial reasoning would be used when assigning a contracted technician for a maintenance job by identifying the doors that leads to the location of the malfunction and granting required physical access.

8.1.3. Visualisation Engine:
The visualisation engine will generate 3D and 2D representations of BIM data to be used by different processes of the authorisation framework such as spatial reasoning and policy transformation. This module will also act as the enforcement point for access control over the BIM elements in visualisation. This can also act as an interface for the users to interact with the building information model at different stages of the authorisation process, such as policy creation based on visual representation and policy simulation and testing. For example, this module can be utilised to visualise access control policies overlayed on BIM visualisation or generate visualisations for the policy transformation module. The command and control operators would be able to use visualisations of BIMs to control all aspects of building operations including granting and revoking access to users.

8.2. Authorisation framework modules

The authorisation framework is conceptually divided into two layers. The authorisation layer includes a Policy Decision Point (PDP), Policy Administration Point (PAP), and Policy Information Point (PIP). This layer adopts the XACML architecture [70] with the main extensions to the XACML standard relating to the additional spatial capabilities of the PDP. The access layer provides service interfaces to external systems to provide and manage access control functions, to both logical and physical resources.

8.2.1. PAP:
The PAP stores and manages policies generated from the policy transformation module. This will be used by the administrators to maintain desired access rights for in a set of policies. It provides managed policies to the PDP for access decision making.

8.2.2. PIP:
The PIP provides external information for access decision-making. This includes information from external sources, such as the spatial reasoning module and other subsystems. The spatial reasoning functions will be provided through an external service to the authorisation framework and it will require an intermediate translation point.

8.2.3. PDP:
A BIM-aware PDP will be able to evaluate access control rules with BIM attributes and spatial functions. This will be in extension of the standard XACML PDP by implementing functionality that would allow making authorisation decisions from BIM specific access restrictions.

8.2.4. Policy Transformation:
The policy transformation module functions as the central entity to generate platform independent access control policies with a spatial dimension for the authorisation framework. It will utilise spatial reasoning to derive the necessary access privileges based on a given criteria. For example, the administrator can grant physical access to a specific space in the building by selecting the initial point of entry and the target space on the BIM visualisation. The spatial reasoning module can analyse the possibility of access between these two points and identify the controlled doors that need to be given access. The transformation module can also identify any conflicts such as the need to pass through an area that requires higher access clearance. The policy transformation module also provides the means to transform and translate high-level platform independent access control policies to the specific formats used by different sub-systems, such as a proprietary physical access control system.

8.2.5. Access Control Interface:
The Access Control Interface will provide access control decision-making capabilities to external systems. Subsystems can use the authorisation framework through this interface to make access control decisions that can then be enforced within the systems. The authorisation framework will be able to handle access requests for both logical and physical resources, thus it provides a unified interface to different systems.

8.2.6. Access Information Interface:
An access information interface will be used to enable external decision making with BIM knowledge. There will be systems that use their own access decision making, such as a proprietary physical access control system. These systems can also use some components of the authorisation layer as external services. For example, an external application can utilise the spatial functions for its own authorisation decision making. A physical access control system that uses its own decision-making functionalities can still use the spatial capabilities and unified policies from the authorisation framework.

8.3. Access control processes

Building information models and associated capabilities can provide new possibilities in three distinct stages of access control. Here we discuss how the framework components interact in each access control process.

8.3.1. Access control policy design

Access control policy design is the process where a security officer of a facility or anyone with delegated privileges creates access control policies that specify which users can access which objects under which conditions and perform which actions. In a simplified form, this can be represented as a quadruple of subject-object-action-condition relationship.

Building information models provide the vocabulary for annotating objects and actions in access control policies. Each object within a building will have a corresponding element in BIM. These BIM objects will also hold attributes that specify actions that can be performed on these objects. For example, the entrance door to a room will be represented in the BIM by a 'door' object with action attributes 'open' and 'close'. Additionally there can be 'conditions' that are based on spatial functions such as connectivity and containment, which require BIMs to specify and compute results.

Building information models also provide a visual user interface for policy creation. The policy transformation module of the authorisation framework will utilise both 'spatial reasoning' and 'visualisation engine' to achieve this. Object and action parts of the access policy quadruple can be selected directly from the visual rendering of a BIM, which will provide the list of selected object and associated actions. Some spatial conditions such as connectivity between spaces can also be visually selected.

8.3.2. Access control management

Once an initial access control policy for a facility is created, it will evolve when new users are added and spaces and objects contained within that are being access-controlled change. Thus, access control management plays an important role in ensuring the effective and correct enforcement of access policies overtime.

Given the objects and actions in policies are from building information models, changes to spaces will be directly reflected in access control policies. The 'visualisation engine' will be use to render policies on top of building spaces and see the changed conditions for visual verification by a security officer. Security officers can also select individual user roles or users and visually check the objects and spaces they have access based on current policy. This will require the use of spatial functions from the both 'spatial reasoning' and 'visualisation engine'.

8.3.3. Access control decision-making

The access control policies generated from the above processes will then be used in decision-making of access control requests. Building information models would enable additional functionality to this process in terms of operating spatial conditional functions on BIMs.

This authorisation framework provides two interfaces that operate in distinct ways of decision-making. The 'access control interface' makes decisions within the framework while the 'access information interface' enables external decision-making with the use of same policies and BIM functions.

The decision making process of the authorisation framework follows the XACML standard with the difference of the ability to use BIM specific spatial function in policies that can be interpreted in 'spatial reasoning' through the 'policy information point'. This enables the use of spatial conditional functions, which can simplify the policy rules.

8.4. Access control policy elements

In all the above access control processes one interconnecting aspect is the access control policy. It is a vital aspect of the authorisation framework and we look at some of the key elements of an access control policy using BIMs.

These policies are used in controlling access to different BIM objects such as building elements and spaces. Most parts of a critical facility and its representation in a BIM may be operationally sensitive so users should only have access when they have a legitimate need. For example, an air-conditioning maintenance operator at an airport would have mobile devices that can access and query BIM server to visualise and view pump and duct locations, but the details of the critical network wirings need not be visible to them. Thus, the visualisation of a building information model needs to be controlled based on the role, assigned tasks (and possibly other contextual factors such as time and location) of the user. The information they can visualise to perform their job must be governed by the access control policy

Objects: In all types of access requests, to both objects within and external of BIMs, they will have corresponding BIM objects to which the access refers. In the case of access to BIM objects, the request would identify the object. For other accesses, such has access to a space, the request would identify the corresponding space object or door object in BIM. Thus, access policies can have a unified way of representing resources. Either they can be IFC class based or individual objects can be represented using their globally unique identifiers (GUID).

Actions: Each access request would specify an action the subject intends to perform of the specified resource.

These actions will vary depending on the type of the resource. For logical resources within a BIM server, create, view, modify, or delete can be typical actions types. For an access request for physical access control to a space, the access type would be to open a given door. Thus, the access policies should be able to support different categories of actions based on the resources.

Conditional functions: The relationships between building elements in a BIM might not necessarily correspond to the physical elements. There can be logical relationships such as zones and ownership. It is useful to have the ability to specify access rules based on these relationships. These can be based on functions that can operate BIM elements as inputs and compute different relationships from the BIM. The following are basic functions that can be used in simplifying policies:

- Contains - Is the requested object contained with an object (space) the user has access to?
- Connected - Is there a physical connection between the two given spaces?
- Adjacent - Are the two given spaces adjacent? If the user has access to both, he can access any connecting objects (doors).
- Accessible - Is the requested space accessible from the current location of the user with his access clearance level?

8.5. Future work and research issues

For future work, we intend to complete the proof-of-concept implementation of an administrative tool utilising the concepts outlined in this paper. This implementation work will be part of the Airport of the Future project [71], based at the Brisbane International Airport, Australia. This implementation will be used to identify the required level of granularity for access control rules. For example, if the access control request is for rendering a floor of the building in visualisation, it can have thousands of individual building elements involved. It is important to analyse the practicality of fine-grained control, which may generate large numbers of requests against the level of security provided by logical groupings.

Providing a formal foundation for the proposed conceptual model will also form the basis of our future work. As a part of this process, we investigate the need for a policy specification language similar to GeoXACML that can address BIM specific requirements. This would require a detailed analysis of existing systems including our prototype implementation to identify the policy elements and spatial functionalities utilising building information models.

9. CONCLUSION

In this paper, we introduced a novel use of Building Information Models for access control. We proposed a new access control framework that unifies policy administration and access control decision making for physical and information resources. We also identified a set of features that are necessary for an authorisation framework that uses building information models. Based on these features, we reviewed the state of the art spatial access control models and established the advantage of building information models for spatiotemporal access control in confined spaces. Finally, we have outlined our future directions to formally define and implement the conceptual authorisation model presented in this paper.

ACKNOWLEDGEMENTS

This research forms part of the work undertaken by the project *Airports of the Future* (LP0990135) which is funded by the Australian Research Council Linkage Project scheme. The authors also acknowledge the contributions made by the many aviation industry stakeholders also involved in this project. More details on *Airports of the Future* and its participants can be found at www.airportsofthefuture.qut.edu.au.

REFERENCES

[1] Ding, L., Drogemuller, R., Akhurst, P., Hough, R., Bull, S., and Linning, C. (2009) Towards sustainable facilities management. In Newton, P., Hampson, K., and Drogemuller, R. (eds.), *Technology, Design and Process Innovation in the Built Environment*, pp. 373–392. Taylor & Francis.

[2] Gollmann, D. (2011) *Computer Security*, 3rd edition. John Wiley and Sons, West Sussex, UK.

[3] Ardagna, C. A., Cremonini, M., Damiani, E., di Vimercati, S. D. C., and Samarati, P. (2006) Supporting location-based conditions in access control policies. *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security, Taipei, Taiwan*, pp. 212–222. ACM, New York, NY, USA.

[4] Bertino, E., Thuraisingham, B., Gertz, M., and Damiani, M. L. (2008) Security and privacy for geospatial data: concepts and research directions. *Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS, Irvine, California*, pp. 6–19. ACM, New York, NY, USA.

[5] Drogemuller, R. and Ding, L. (2007) Automated code checking and accessibility. In Aouad, G., Lee, A., and Wu, S. (eds.), *Constructing the Future: nD Modelling*. Taylor & Francis.

[6] Filippoupolitis, A. and Gelenbe, E. (2009) A distributed decision support system for building evacuation. *Proceedings of the 2nd conference on Human System Interactions*, Piscataway, NJ, USA HSI'09, pp. 320–327. IEEE Press.

[7] Gorbil, G., Filippoupolitis, A., and Gelenbe, E. (2012) Intelligent navigation systems for building evacuation. In Gelenbe, E., Lent, R., and Sakellari, G. (eds.), *Computer and Information Sciences II*, pp. 339–345. Springer London.

[8] Contos, B. T., Derodeff, C., Crowell, W. P., and Dunkel, D. (2007) *Physical and Logical Security Convergence: Powered By Enterprise Security Management*. Syngress Publishing.

[9] Mehdizadeh, Y. (2003) Convergence of logical and physical security. Technical report. SANS Institute, Bethesda, MD, USA.

[10] Melendez, J. C., Luse, A., Townsend, A. M., and Mennecke, B. (2008) Convergence of physical and logical security: A pre-implementation checklist. *Proceedings of MWAIS 2008, Eau Claire, WI, USA*, 23-24 May. Association for Information Systems, Atlanta, GA, USA.

[11] Fernandez, E. B., Ballesteros, J., Desouza-Doucet, A. C., and Larrondo-Petrie, M. M. (2007) Security patterns for physical access control systems. *Proceedings of the 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security, Redondo Beach, CA, USA*, pp. 259–274. Springer-Verlag, Berlin, Heidelberg, Germany.

[12] Yang, L. and Worboys, M. (2011) Similarities and differences between outdoor and indoor space from the perspective of navigation. *Accepted poster. Conference on Spatial Information Theory, Belfast, ME, USA*.

[13] Yang, L. and Worboys, M. (2011) A navigation ontology for outdoor-indoor space: (work-in-progress). *Proceedings of the 3rd ACM SIGSPATIAL International Workshop on Indoor Spatial Awareness, Chicago, Illinois* ISA '11, pp. 31–34. ACM, New York, NY, USA.

[14] El-Mekawy, M., stman, A., and Shahzad, K. (2011) Towards interoperating CityGML and IFC building models: A unified model based approach. In Kolbe, T. H., Knig, G., and Nagel, C. (eds.), *Advances in 3D Geo-Information Sciences* Lecture Notes in Geoinformation and Cartography, pp. 73–93. Springer Berlin Heidelberg.

[15] Portele, C. (2012) OGC Geography Markup Language (GML) – Extended schemas and encoding rules. Technical Report OGC 10-129r1. Open Geospatial Consortium Inc.

[16] Grger, G., H. Kolbe, T., Nagel, C., and Hfele, K.-H. (2012) OGC City Geography Markup Language (CityGML) Encoding Standard. Technical Report OGC 12-019. Open Geospatial Consortium Inc.

[17] Worboys, M. (2011) Modeling indoor space. *Proceedings of the 3rd ACM SIGSPATIAL International Workshop on Indoor Spatial Awareness, Chicago, Illinois* ISA '11, pp. 1–6. ACM, New York, NY, USA.

[18] Li, K.-J. (2008) Indoor space: A new notion of space. In Bertolotto, M., Ray, C., and Li, X. (eds.), *Web and Wireless Geographical Information Systems*, Lecture Notes in Computer Science, **5373**, pp. 1–3. Springer Berlin / Heidelberg.

[19] Li, K.-J. and Lee, J. (2010) Indoor spatial awareness initiative and standard for indoor spatial data. *Proceedings of IROS 2010 Workshop on Standardization for Service Robot, Taipei, Taiwan*, October IROS '10.

[20] Nagel, C., Becker, T., Kaden, R., Li, K.-J., Lee, J., and Kolbe, T. H. (2010) Requirements and space-event modeling for indoor navigation. Technical Report OGC 10-191r1. Open Geospatial Consortium Inc.

[21] Open Geospatial Consortium (2012). OGC IndoorGML 1.0 Standard Working Group. Online, Available from: http://www.opengeospatial.org/projects/groups/indoorgmlswg.

[22] Liebich, T., Adachi, Y., Forester, J., Hyvarinen, J., Karstila, K., Reed, K., Richter, S., and Wix, J. (2010). buildingSMART: Industry Foundation Classes, IFC2x Edition 4 Release Candidate 2. Online, Available from: http://buildingsmart-tech.org/.

[23] Schlueter, A. and Thesseling, F. (2009) Building information model based energy/exergy performance assessment in early design stages. *Automation in Construction*, **18**, 153–163.

[24] Succar, B. (2009) Building information modelling framework: A research and delivery foundation for industry stakeholders. *Automation in Construction*, **18**, 357 – 375.

[25] Gu, N., Singh, V., Taylor, C., London, K., and Brankovic, L. (2010) Bim adoption: Expectations across disciplines. *Handbook of Research on Building Information Modeling and Construction Informatics: Concepts and Technologies*, pp. 501 – 520. IGI Global.

[26] Peck, R. L. (2011) BIM The game-changer. *Healthcare Design*, **11**, 29–32.

[27] Baty, J. (2012) The Rise of BIM. *Concrete Contractor*, **12**, 34–37.

[28] Steel, J., Drogemuller, R., and Toth, B. (2010) Model interoperability in building information modelling. *Software and Systems Modeling*, **11**, 99–109.

[29] Nagel, C., Stadler, A., and Kolbe, T. H. (2009) Conceptual requirements for the automatic reconstruction of building information models from uninterpreted 3D models. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, **34**, 46–53.

[30] Ansari, S., Rajeev, S., and Chandrashekar, H. (2002) Packet sniffing: a brief introduction. *IEEE Potentials*, **21**, 17–19.

[31] Igure, V. M., Laughter, S. A., and Williams, R. D. (2006) Security issues in SCADA networks. *Computers and Security*, **25**, 498 – 506.

[32] Byres, E. and Lowe, J. (2004) The myths and facts behind cyber security risks for industrial control systems. *Proceedings of VDE Congress*. VDE Association for Electrical, Electronic and Information Technologies.

[33] Dimakis, N., Filippoupolitis, A., and Gelenbe, E. (2010) Distributed building evacuation simulator for smart emergency management. *The Computer Journal*, **53**, 1384–1400.

[34] Gelenbe, E., Hussain, K., and Kaptan, V. (2005) Simulating autonomous agents in augmented reality. *Journal of Systems and Software*, **74**, 255–268.

[35] Ferraiolo, D. F. and Kuhn, D. R. (1992) Role-based access controls. *Proceedings of the 15th National Computer Security Conference, Baltimore, MD, USA*, pp. 554–563. NIST/NSA.

[36] Chapin, P. C., Skalka, C., and Wang, X. S. (2008) Authorization in trust management: Features and foundations. *ACM Computing Surveys*, **40**, 9:1–9:48.

[37] Covington, M. J., Moyer, M. J., and Ahamad, M. (2000) Generalized role-based access control for securing future applications. *Proceedings of the National Information Systems Security Conference*, October.

[38] Atluri, V. and Chun, S. A. (2004) An authorization model for geospatial data. *IEEE Transactions on Dependable and Secure Computing*, **1**, 238–254.

[39] Bertino, E., Catania, B., Damiani, M. L., and Perlasca, P. (2005) GEO-RBAC: a spatially aware RBAC. *Proceedings of the 10th ACM Symposium on Access Control Models and Technologies, Stockholm, Sweden* SACMAT '05, pp. 29–37. ACM, New York, NY, USA.

[40] Ray, I. and Toahchoodee, M. (2007) A spatio-temporal role-based access control model. *Proceedings of the 21st annual IFIP WG 11.3 working conference on Data and applications security, Redondo Beach, CA, USA*, pp. 211–226. Springer-Verlag, Berlin, Heidelberg.

[41] Samuel, A., Ghafoor, A., and Bertino, E. (2007) A framework for specification and verification of generalized spatio-temporal role based access control model. Technical Report CERIAS-TR-2007-08. Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, IN, USA.

[42] Aich, S., Mondal, S., Sural, S., and Majumdar, A. K. (2009) Role based access control with spatiotemporal context for mobile applications. *Transactions on Computational Science IV: Special Issue on Security in Computing*, **5430**, 177–199.

[43] Matheus, A. and Herrmann, J. (2008) Geospatial eXtensible Access Control Markup Language (GeoXACML). Technical Report 07-026r2. Open Geospatial Consortium Inc.

[44] Sandhu, R. S., Coyne, E. J., Feinstein, H. L., and Youman, C. E. (1996) Role-based access control models. *Computer*, **29**, 38–47.

[45] Sandhu, R., Ferraiolo, D., and Kuhn, R. (2000) The nist model for role-based access control: towards a unified standard. *Proceedings of the fifth ACM workshop on Role-based access control, Berlin, Germany* RBAC '00, pp. 47–63. ACM, New York, NY, USA.

[46] Li, N., Tripunitara, M. V., and Bizri, Z. (2007) On mutually exclusive roles and separation-of-duty. *ACM Transactions on Information and System Security*, **10**.

[47] Ferraiolo, D. F., Sandhu, R. S., Gavrila, S. I., Kuhn, D. R., and Chandramouli, R. (2001) Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security*, **4**, 224–274.

[48] Kuhn, D. R., Coyne, E. J., and Weil, T. R. (2010) Adding attributes to role-based access control. *Computer*, **43**, 79–81.

[49] Thomas, R. K. and Sandhu, R. S. (1993) Discretionary access control in object-oriented databases: Issues and research directions. *Proceedings of the 16th NIST-NCSC National Computer Security Conference, Baltimore, MD, USA*, September, pp. 63–74.

[50] Bertino, E., Bettini, C., and Samarati, P. (1994) A discretionary access control model with temporal authorizations. *Proceedings of the 1994 workshop on New security paradigms, Little Compton, Rhode Island, USA*, pp. 102–107. IEEE Computer Society Press, Los Alamitos, CA, USA.

[51] Neuman, B. and Ts'o, T. (1994) Kerberos: an authentication service for computer networks. *IEEE Communications Magazine*, **32**, 33–38.

[52] Bertino, E., Bettini, C., Ferrari, E., and Samarati, P. (1996) A temporal access control mechanism for database systems. *IEEE Transactions on Knowledge and Data Engineering*, **8**, 67–80.

[53] Bertino, E., Bettini, C., Ferrari, E., and Samarati, P. (1998) An access control model supporting periodicity constraints and temporal reasoning. *ACM Transactions on Database Systems*, **23**, 231–285.

[54] Samarati, P. and de Vimercati, S. (2001) Access control: Policies, models, and mechanisms. *Foundations of Security Analysis and Design*, Lecture Notes in Computer Science, **2171**, pp. 137–196. Springer, Berlin, Heidelberg, Germany.

[55] Herrmann, J. (2011) Administration of (geo)xacml policies for spatial data infrastructures. *Proceedings of the 4th ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS, Chicago, Illinois* SPRINGL '11, pp. 53–59. ACM, New York, NY, USA.

[56] Damiani, M. L., Silvestri, C., and Bertino, E. (2008) Hierarchical domains for decentralized administration of spatially-aware rbac systems. *Proceedings of the Third International Conference on Availability, Reliability and Security, Barcelona, Spain*, 4-7 March ARES '08, pp. 153–160. IEEE Computer Society, Washington, DC, USA.

[57] Damiani, M. L. and Silvestri, C. (2008) Towards movement-aware access control. *Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS, Irvine, California* SPRINGL '08, pp. 39–45. ACM, New York, NY, USA.

[58] Bonatti, P., de Capitani di Vimercati, S., and Samarati, P. (2000) A modular approach to composing access control policies. *Proceedings of the 7th ACM conference on Computer and communications security, Athens, Greece* CCS '00, pp. 164–173. ACM, New York, NY, USA.

[59] OGC 99-049 (1999) Open GIS simple features specification for SQL. revision 1.1. Technical Report. Open GIS Consortium.

[60] Kirkpatrick, M. S., Damiani, M. L., and Bertino, E. (2011) Prox-RBAC: a proximity-based spatially aware RBAC. *Proceedings of the 19th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems, Chicago, Illinois* GIS '11, pp. 339–348. ACM, New York, NY, USA.

[61] Damiani, M. L., Bertino, E., Catania, B., and Perlasca, P. (2007) GEO-RBAC: A spatially aware RBAC. *ACM Transactions on Information and System Security*, **10**.

[62] Damiani, M. L., Bertino, E., and Silvestri, C. (2008) Spatial domains for the administration of location-based access control policies. *Journal of Network and Systems Management*, **16**, 277–302.

[63] Ray, I. and Toahchoodee, M. (2008) A spatio-temporal access control model supporting delegation for pervasive computing applications. *Trust, Privacy and Security in Digital Business*, Lecture Notes in Computer Science, **5185**, pp. 48–58. Springer, Berlin, Heidelberg, Germany.

[64] Joshi, J. B., Bertino, E., Latif, U., and Ghafoor, A. (2005) A generalized temporal role-based access control model. *IEEE Transactions on Knowledge and Data Engineering*, **17**, 4–23.

[65] Aich, S., Sural, S., and Majumdar, A. K. (2007) STARBAC: spatiotemporal role based access control. *Proceedings of the 2007 OTM Confederated International Conference on On the Move to Meaningful Internet Systems, Vilamoura, Portugal* OTM'07, pp. 1567–1582. Springer-Verlag, Berlin, Heidelberg, Germany.

[66] Matheus, A. (2005) Declaration and enforcement of fine-grained access restrictions for a service-based geospatial data infrastructure. *Proceedings of the 10th ACM Symposium on Access Control Models and Technologies, Stockholm, Sweden* SACMAT '05, pp. 21–28. ACM, New York, NY, USA.

[67] Lin, J., Fang, Y., and Chen, B. (2008) Using saml callout to realize access restriction for geospatial grid services. *Proceedings of the Seventh International Conference on Grid and Cooperative Computing, Shenzhen, China*, October, GCC '08, **7**, pp. 583–588. IEEE Computer Society, Washington, DC, USA.

[68] Kolovski, V., Hendler, J., and Parsia, B. (2007) Analyzing web access control policies. *Proceedings of the 16th international conference on World Wide Web, Banff, Alberta, Canada* WWW '07, pp. 677–686. ACM, New York, NY, USA.

[69] Anderson, A. (2005) Core and hierarchical role based access control (RBAC) profile of XACML Version 2.0. OASIS Standard. Technical report. OASIS Open.

[70] Moses, T. (2005) eXtensible Access Control Markup Language (XACML) Version 2.0. OASIS Standard. Technical report. OASIS Open.

[71] Queensland University of Technology (2012). Airports of the Future. Online, Available from: http://www.airportsofthefuture.qut.edu.au/.