Security Model Collaborative Building Design

Kaznah Alshammari,
Cardiff University
(email: alshammarik1@cardiff.ac.uk)
Prof. Haijiang Li,
Cardiff University
(email: lih@cardiff.ac.uk)
Prof. Alan Kwan,
Cardiff University
(email: kwan@cardiff.ac.uk)

Abstract

This research concerns the topic of Building Information Modelling (BIM), data governance and security frameworks directed towards finding an appropriate method to security model a collaborative building design. This is concerned with knowledge of the structure and model of information that is utilised in the collaborative building design, the security threats that face the structure and model of information and concerning information security to achieve the stated goal.

BIM implementation has benefits associated with the BIM process. These benefits include the flexibility of workflow and that performance in collaboration can be facilitated to model data integration. Team members can work uninterrupted on the same model. However, there are certain steps that can be taken to control the model and manage it without inconsistencies arising. Some of these steps include assigning users to a workstation so that others are prevented from making changes to features at the same time. In addition, when a modification is made, a copy of the system must be synchronised with the local copy in order to achieve intergradation with the central model of BIM. The collaboration problem was not complex prior to BIM because the participants would simply work on different sheets. BIM effectively processes the inefficiencies and inaccuracies of the traditional methods at a cost of reduced flexibility and an increase in collaboration complexity. Problems can arise when an application has a centralised model of approach because most files are contained in a single file.

Having understood the information model and related security threats, the model proposed to secure the BIM for a collaborative building design is developed to prioritise the security of all information exchanged between the involved parties. The security model that is proposed addresses security concerns: protection of building information from access by unauthorised individuals and the creation of information in the BIM through unauthorised access.

The security model allows for the arrangement of data according to measures put in place according to the classification of information in the BIM. The model also records the activities of users to enable any breach to be traced to a particular user. The model uses these user activity records and defines patterns and best practices that reduce the probability of information compromise in the BIM. Many security models only store information and place little emphasis on protection or the access that users are granted to this information.

Keywords: BIM, collaborative building design, information security, access controls and multi-layered security.

1. Introduction

In the modern world, the construction industry creates amazing architecture and seemingly impossible building designs such as the tallest building in the world which is currently the Burj Khalifa in the United Arab Emirates. Such architecture requires considerable input and effort, whereas more is expected from the well informed consumer. Such an environment in the construction industry calls for the implementation of a technology and information basis. All of the stakeholders involved in projects are to keep abreast of the latest information and direction of the projects. It requires competent coordination and collaboration in a concept that has come to be defined as collaborative building designing (Chen et al., 2005). Such a collaborative environment demonstrates an increased security threat regarding the information exchanged and accessed by the numerous stakeholders directly involved. Information is very valuable and is always at risk on account of the modern threats to the security of information.

Information security challenges have been a problem for collaborative organisations for long as information models have existed. Collaborative environments in the construction industry have faced growing cases of information security breaches that have been known to bring projects to a complete standstill. Management has struggled to tackle information breaches, loss and information system damage. Few have been able to recover from the problem and resume normal business operations or carry out a complete turnaround to install and integrate new, safer information models and provide better services to their consumers (Merkow & Breithaupt, 2014).

The increase in cases of information breaches are attributed to a lack of accurate understanding about information models by management that initially result in the establishment of poor information models that are highly susceptible to attacks, theft, hacking, and unintentional mistakes by internal personnel. The effects of misunderstood information model management among management boards include the failure of organisations to stay up-to-date with the respective information model and constantly manage their systems to ensure they are safe from attack, theft and error that may lead to problems (Ifinedo, 2011).

The aim of this paper is to create an appropriate security model for a collaborative building design in the construction industry. The security model that is proposed addresses security concerns relating to the protection of building information and also information in the BIM from access by unauthorised individuals. This security model depends on a three layer approach to deal with access based security for building management information. The security model takes into account the arrangement of data as per measures set up for the classification of information in the BIM. The model likewise records the activities of users to enable any breach to be traced to a specific user. The model uses these user activity records and characterises patterns and best practices that reduce the risk of information being compromised in the BIM. Therefore, the proposed model has the features required to realise successful security for building information models.

The paper is organised as follows: in Section 2, related works define the building information model, collaborative building design, and information system security; Section 3 sets out the methodology for the proposed security model collaborative building design, and security model development; Section 4 presents the results and provides a discussion; while Section 5 concludes.

2. Related work

2.1 Building information model

Architecture, engineering and construction (AEC) create and design three dimensions (3D) modelling using BIM software which is a platform that makes the communication of project ideas and design easier. It also provides tools for buildings and infrastructure that contain big data and allows the exchange of BIM data between BIM users (Autodesk, 2003).

Autodesk "Revit" is a type of BIM software intended for architecture, structure and mechanical, electrical, and plumbing (MEP). It is a strong development platform that enables architects and engineers to plan and design a building and its elements in 3D. It also enables comments to be added to the model with two dimensions (2D) drafting components and access building data from the model database. Revit is 3D plus time schedule (4D BIM) which as a tool is used to plan and design all parts of a building project from construction to demolition. Additionally, the Revit interface supports various methodologies for utilising the Revit. Therefore, it provides a high level of elasticity for architects and designers. Autodesk "Revit" does not run on all operating systems, e.g. the Apple Macintosh operating system (OSX). Because the file size is expandable, Autodesk "Revit" needs to fasten to a central processing unit (CPU). Autodesk "Revit" is an import and export tool for common types of files containing 3D models, 2D drawings and other types of file ("Which BIM software is better? ArchiCAD vs Revit? - Cadonia", 2019).

Autodesk "Revit” contains several tools offering specific functions used by Revit users (engineers and architectures) to create and design buildings (Lee & Wu, 2005). The tools in Autodesk "Revit” are not just to create and design, they also serve the BIM group by exchanging BIM data and are connected between them. Autodesk "Revit” permits a link with a BIM database by using an existing plugin called ‘Revit DB link’ (Autodesk, 2003).

BIM data in database can be stored through the Revit interface using the existing plugin with Revit called ‘Export.’ Additionally, Autodesk "Revit” deals with certain software and folders (e.g. Microsoft SQL server management and Visual studio.NET software; Integration service script component; custom office template) to add new features by using the existing plugin with Revit called ‘File Data Source.’

The BIM method is built for design, construction and project management. It also stores and retrieves big data in the BIM database. Therefore, project teams have a database structure to link it with BIM project data. BIM modelling utilises existing commercial software such as Revit (Autodesk), Constructor (Microsoft) and Microstation (Bentley). Each piece of software connects with a unique BIM database to store and retrieve big data for the BIM project. Autodesk “Revit” uses an existing plugin with Revit that relates types of files to the BIM database (Cha & Lee, 2015).

2.2 Collaborative Building Design

Modern technology has brought about numerous changes in the construction industry and the industry is no longer merely physical but rather data-based. The industry has taken a turn towards the inclusive involvement of all stakeholders in a development project or a real estate project coming up with a certain facility. The modern construction industry requires a constant transaction of information and data. This data is key to ensuring that all members of a project team understand the direction the project is taking. To bring all this information to a common access and effectively engage in BIM, there is a need for the effective collaboration and coordination of data, as shown in Figure 1 (Chen et al., 2005). All of this data is very important and needs to be secured. This calls for the development of effective security models for collaborative building design.

When implementing the BIM, there are benefits associated with this process but that does not mean that they are necessarily achieved. Some of the benefits include flexible workflow and even the performance in collaboration can be reduced to model data integration. Team members can work uninterrupted on the same model. However, there are certain steps that can be taken in order to control the system and manage it without any inconsistencies. These steps include assigning users a workstation so that other users can’t make changes to features at the same time. Simultaneously, when changes are made, it is necessary to update or synchronise the system using a local copy to ensure a connection with the central BIM model.

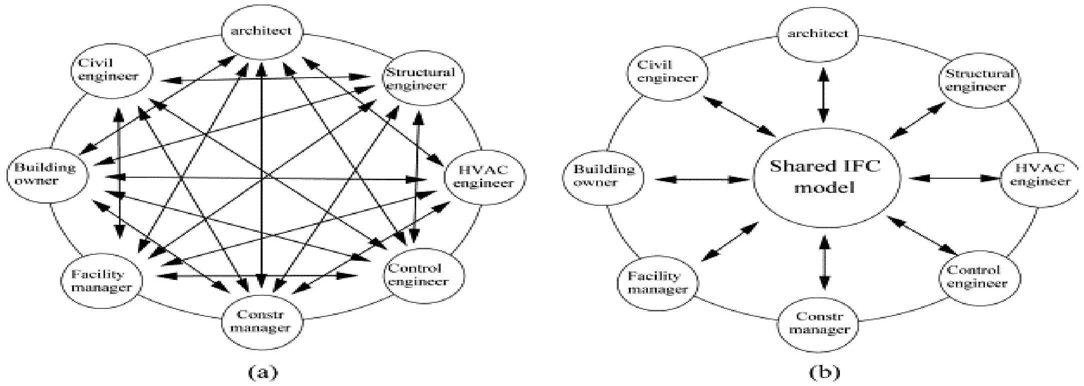

Figure 1 Collaborative building design information flow (Chen et al., 2005).

Most BIM has flexibility limitations which affects the collaborative style in the organisation. As a result, the software is affected by the trade-off between workflow flexibility and the barriers set in collaborative performance. An increase in data integration is met with reductions in both performance and workflow flexibility. It is necessary to actively manage the changes being made by the various members of a project team when they are working concurrently because failure to do so will result in conflict (Teamwork & Ipd, 2009).

In this case, the architects and engineers need to work together in order to accomplish the best outcome and utilisation of a building. As architects become increasingly aware, they specialise and projects become more complex. The design disciplines when working on the same building remain with workers using their own sets of tools and practices (Sacks, Koskela, Dave, & Owen, 2010). This makes the common issues experienced in communication and coordination in a normal office set up no different in this area. In construction, collaboration can be understood as the internal and external processes that occur when the users who edit or modify a model within or outside the organisation do so simultaneously. Sacks, Koskela, Dave, & Owen, (2010) noted that whereas it is possible to lock away internal objects to prevent irregularities when they are edited to create additional versions, when utilising the external method, it is only the representations that are shared and cannot be edited. This mitigates the problem but has the effect of making it necessary for the various disciplines to each amend their specific objects.

The collaboration problem is not complex prior to BIM because the participants would simply work on different sheets. BIM effectively handles the problematic inefficiencies and inaccuracies of the traditional methods at a cost of less flexibility and an increase in collaboration complexity. Therefore, in this case the collaboration problem is more complex following the introduction of BIM because the multidisciplinary team members have to work in a synchronised model. The problem intensifies when an application has a centralised model of approach because most of the files are contained in one file.

2.3 Information system security

Information security is a collection of practices that prevent unauthorised access, disclosure, use and modification. Information security refers to the security of the components of the information model (Whitman & Mattord, 2017). These include hardware security, software security and personal security. Information security needs can be expressed in four main categories. These ideas ensure that information security is maximised by preserving confidentiality, integrity, availability, and configuration in an information system (Kim & Solomon, 2018).

Information confidentiality: determining who has access to information so as to ensure that unauthorised persons cannot gain access to sensitive or classified information.

Information integrity: ensuring compliance with procedures concerning how information is modified and deleted.

Information system availability: ensuring that access is only granted to authorised persons and that they use the information in accordance with the stated policies.

System configuration: ensuring that an information system's configuration settings can only be changed by those who are authorised to do so in accordance with the stated system modification guidelines.

3. Methodology

3.1 Proposed Security Model Collaborative Building Design

Upon understanding the information system security threats (including viruses, spam and internal theft of information), the model that is proposed to secure the BIM for a collaborative building design is developed to prioritise the security of all information exchanged between the parties involved using secure communication, classification and authorisation of access and prioritising the security of the host cloud. The model proposed is a dedicated system for the storage of building information systems. This model was not implemented to store and secure personally identifiable information; rather, building information exchanged in a collaborative building design such as agreements, intellectual property, financial information relating to projects and contracts.

The security model that is proposed addresses two significant security concerns:

- Protection of the building information from access by unauthorised individuals and any creation of information in the BIM by the unauthorised persons.

- The security model also ensures that there is information available to authorise access within a hosted cloud environment. It provides prompts and guides to successfully complete the task at hand and uses the authority level of the user to access information instead of leaving the user with the task of going through stored archives to obtain the information required for the task at hand.

Figure 2 shows a multi-layered approach to ensure the security of the collaborative building design information to address these two concerns.

3.1.1 Layers of the proposed security model collaborative building design

First layer of the security model: The building information context and the classification of the building information data that support information security.
Upon the data interchanged in the collaborative building design being classified, the building information will be stored in the security system based on sensitivity and criticality. This information is a confidential building information system and strictly not individual sensitive data.

The proposed security model classifies the information in the BIM (see Table 1). The security model then uses this classification to make authorisation levels based on the needs of the collaborative building environment stakeholders. The authorisation levels are customised to each collaborative environment from the lowest to the highest in hierarchy. The entities in the authorisation level will require authority to access information above their level.

The classification is as follows:

Pubic information: This information is available to the general public such as occupational opportunities in the project. Compromises information that has no impact on the security of the BIM.

Employee confidential: This includes standards, guidelines, procedures and processes utilised in the building information. Compromises information that could cause harm to the organisation including the exposure of competitive advantages.

Non-disclosure agreement (NDA) confidential information: This includes documents that are only accessed by stakeholders with non-disclosure, including agreements and contracts relating to collaborative building design. Compromise of such information would inflict significant damage to collaborative building design.

Insider restricted information: Such information includes intellectual property, project plans and financial data. This data is only accessible by people who have signed an agreement never to disclose any information that is top secret for the BIM.

Private information: Personally identifiable information such as financial records that are only accessible by the owner of the information. Any compromise could lead to a loss of credibility for a project.

Table 1 Classification of the information in the BIM

Classification	Colour Code (Model Diagram)	Impact of compromise
Public	🟦	None
Employee Confidential	🟩	Limited
NDA Confidential	🟨	Significant
Insider Restricted	🟫	Significant
Private	🟧	Serious

Second layer of the security model: Controls built into the system that are customised to the collaborative building design environment.

These security controls are developed to fit the specific requirements of different collaborative building designs and secure the building information interchanged by stakeholders. These user requirements for collaborative building designs include user identification, user specifications for the security model, user designs and interfaces that will be integrated into the security model.

The controls include:

Access controls: The access controls secure the BIM. Access is only allowed to assigned users given permission to access and execute the function of the system including the creation records and retrieval of data. Any compromised access triggers will result in account lockout based on the specified rules.

Version control: This control keeps a tab on the edits made to the BIM. These changes are traced back to an individual user and, therefore, provide accountability. The security model logs the activities of each user and the information they input into the BIM. The changes are tracked to the specific users.

The information that existed (prior version of the information) is stored and archived. The prior version of the edited data is archived in the security system for retrieval by those with prioritised access.

Audited logging: Audit trails are created by the security system for all activities by an assigned individual with authorised access. This control also establishes accountability and monitors the performance of stakeholders in the collaborative building design environment. The application of audited logging in the security model is to maintain a record of each activity performed by the users and, therefore, trace back any breach of information to the user ID and manage the threat.

Third layer of the security model: practical security.

Development cycle of security: The system allows for the development of customised security models from configuration to final implementation. This ensures that the requirement of different collaborative environments is met.

Depth of defence: Multi-layered security will be utilised in the proposed model within collaborative environments, as elaborated in Figure 2. There will be multi-tenanted network segments in between the internet and the system and all data for the BIM entailing public to private information as specific to the classification of information in the security model.

Patch management: New threats to information security are introduced into the construction industry each day. This calls for the implementation of security measures to sufficiently protect building information in collaborative environments. Patch management will be the responsibility of the providers of the security model to maintain the system and continually update the security measures. This function will test and install multiple code changes to continually secure the BIM against new security threats.

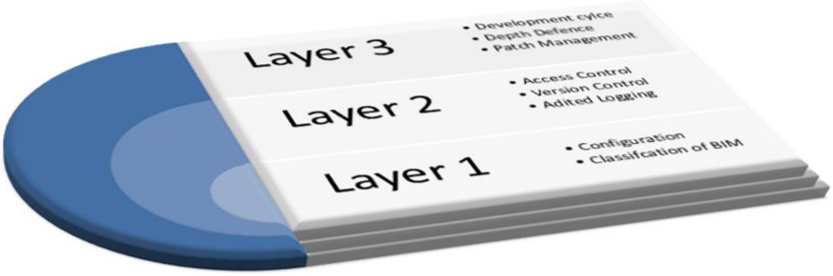

Figure 2: Proposed security model Collaborative building design

3.2 Security model development

The security model proposed will utilise C# which is a very powerful programming language that has been put to various uses in modern technology. The security model proposed will effectively use a three layer design to carry out access clearance based security for building management information in a Structured Query Language (SQL) server database system. The security model will comprise the following layers: User interface layer (Layer 1), Business logic layer (Layer 2) and Database access layer (Layer 3).

The multi-layered approach helps to ensure that change management is able to be implemented. Changing content in the business logic layer, for example after some period of use, will not affect the database access layer or the user interface layer. C# will be utilised to develop the three layers of the security model, whereas further security shall be provided by the Advanced Encryption Standard for sensitive data.

User interface layer: The user interface layer will be simple to use and graphical to help users. This layer will contain the web forms for web-based applications.

Business logic layer: This layer will essentially contain the specific areas or rather part of the system that will create the logical or business rules for access to, and creation and modification of the data. It will allow these functions based on user clearance and access controls in the system. The business logic layer will have functions such as access control, version control and audited login. C# will create parameters that will only allow the user to process from the business logic layer (layer 2) to the data access layer (layer 3) given that the SQL query of the clearance and the stored procedure of access remains true. The version control will allow the creation and modification of data in the SQL server database (DB) given that clearance and the stored procedure of access remains true. The audited login will keep records for user access into the data access layer through the business logic layer to track user activity in the security model.

Data Access Layer: The database that the system will be utilising is the SQL server. Data access prevents authorisation by managers, owners and the board depending on their clearance level.

4. Results and discussion

BIM Design collaboration is new phenomenon to the AEC industry. There is not a secure model for BIM that facilitates a collaborative approach to designing buildings while ensuring the security of the information exchanged by those involved in the process when discussing matters such as intellectual property, agreements, contracts and financial information. Consequently, this research proposes a security model based on a three layer approach to deliver access clearance based security for building management information.

This research has delivered a security model collaborative building design of BIM that can improve the information security of BIM for stakeholders. It integrates a BIM collaborative building design and information security to help secure the design process of BIM based on the amalgamation of control access and BIM data. It enables communication between stakeholders with a high security model and team members can work uninterrupted on the same model.

The security model collaborative building design that is proposed in this paper to manage BIM information in collaborative building designs involves version control, access control and audited logging. Adopting such an approach ensures that only authorised users are able to access and perform the function. Any previous versions of the data are stored within the security system so that they can be retrieved if needed at a later date with the changes made by each individual being logged.

The security model also comprises the user interface layer, business logic layer and the database access layer. It is this multi-layered approach that enables change management to be delivered. For instance, making changes to the business logic layer’s content has no effect on either the user interface layer or the database access layer. All three layers of the security model will be developed using C#, with additional security to protect particularly sensitive data being delivered by the Advanced Encryption Standard (AES).

The security model collaboration building design on BIM can be validated by experts in terms of the accuracy and completeness of the data and the effectiveness of the security model.

5. Conclusion

Security is a very important aspect in constantly changing collaborative building designs with numerous stakeholders required to access and generate information for useful outcomes. This research implements a holistic approach that makes allowance for the security threats facing collaborative BIM to develop a security model that reflects the security risks that challenge collaborative environment information in the construction industry. The proposed model has the features required to enable effective security for BIM.

6. Acknowledgements

The author acknowledges the Northern Border University, Saudi Arabia for the assistance offered. However, the opinions and statements presented in this paper are purely those of the author and are not necessarily endorsed by the University.

7. References

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

Which BIM software is better? ArchiCAD vs Revit? - Cadonia. (2019). Retrieved from http://cadonia.com.au/which-bim-software-is-better-archicad-or-revit.

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

Chen, P., Cui, L., Wan, C., Yang, Q., Kiong, S., & Tiong, R. L. K. (2005). Implementation of IFC-based web server for collaborative building design between architects and structural engineers, *14*, 115–128. https://doi.org/10.1016/j.autcon.2004.08.013.

Kim, D., & Solomon, M. (2018). *Fundamentals of information systems security* (3rd ed., Chapter 4).

Ifinedo, P. (2011). Understanding information systems security policy compliance : An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007.

Lee, A., & Wu, S. (2005). The utilisation of Building Information Models in modelling: A study of data interfacing and adoption barriers, *10*(February), 85–110.

Merkow, M. S., & Breithaupt, J. (2014). *Information Security: Principles and Practices* (2nd ed., Chapter 2).

Sacks, R., Koskela, L., Dave, B. A., & Owen, R. (2010). Interaction of Lean and Building Information Modeling in Construction, *136*(September), 968–980.

Teamwork, G., & Ipd, B. I. M. (2009). NEXT-GEN BIM :, (25).

Whitman, M. E., & Mattord, H. (2017). Principles of Information Security, (January 2005).