Cybersecurity Management Framework for a Cloud-Based BIM Model

39

Ivan Mutis and Anitha Paramashivam

Abstract

Today, building information models (BIM) are developed independently among participating project stakeholders, often using independent technology platforms. Integrating the information these models convey into one standalone system results in substantial challenges. It hinders the stakeholders' use of a shared and common platform, thereby restricting access to a common data environment (CDE). These problems lead to inefficiencies in managing the information exchange process among the actors throughout a project's lifecycle. Cloud computing has emerged as a new model for hosting and delivering services over the internet. This model has rapidly altered the methods by which information technology is used to meet today's demand for economically efficient, powerful, and ubiquitously available computer resources. The model promises a technology transformation across the highly interconnected business environments of the architecture, engineering, and construction (AEC) industry. Integrating Cloud computing and BIM technologies is the next generation of BIM development and will further pervade the adoption of BIM in the AEC industry, thereby incorporating new forms of collaboration amongst project stakeholders. Cloud-BIM implementation overcomes the natural limitations of standalone models in multiple ways. Benefits include reducing up-front investments in computer resources, lowering operating and maintenance costs through on-demand service allocation, enabling rapid scalability of computing, and enhancing and facilitating rapid access, to name several benefits. Cloud-BIM models enable distributed and highly intensive data transactions among project actors; however, a new way of operating and transacting, they bring with them challenges related to security management. For instance, data redundancy occurs when multiple instances of the same data exist, and it leads to problems of inconsistency (i.e., identical fields having different or multiple values) where an update is not reflected in all fields. A Cloud-BIM model provides a central access point to the project actors, safeguards data and promotes data consistency by helping to avoid redundant data and promote positive types of data redundancy. Another major challenge is the data breach that involves leaks of information not intended for public release. Data breach is the result of application vulnerabilities, human error, and/or poor security practices. The most common types of security challenges in cloud computing are addressed by this research.

Keywords

BIM • Cloud computing • Cloud-based BIM • Cloud security • BIM Cloud integration

I. Mutis · A. Paramashivam (✉)
Department of Civil and Architectural Engineering, Illinois Institute of Technology, Chicago, IL, USA
e-mail: aparamashivam@hawk.iit.edu

I. Mutis
e-mail: imutissi@iit.edu

I. Mutis and T. Hartmann (eds.), *Advances in Informatics and Computing in Civil and Construction Engineering*,
https://doi.org/10.1007/978-3-030-00220-6_39

39.1 Introduction

Adoption of Cloud-based Building Information Modelling (BIM) in the architecture, engineering, and construction (AEC) industry results in the development of efficient collaborative workflows among the different disciplines involved in the lifecycle of a construction project. Cloud computing directly benefits BIM and is emerging in the IT sector for its efficient web-based data exchange and storage. The effective integration of cloud computing and BIM is the focus of recent research. BIM provides automation capabilities for more integrated communication, data exchange and sharing between project actors within a virtual 3D environment ([11] #118). Large amounts of data are generated during the life cycle of a construction project and are stored in the centralized, accessible repository for usage. The concept of a centralized repository is important as it forms a framework to manage the process of data generation and exchange between all project members and stakeholders ([23] #2). It is highly challenging to handle data in collaborative work environments while ensuring security, privacy, and protection against other IT risks. Privacy, risk, and Cybersecurity concerns, however, continue to impede the widespread adoption of Cloud-based BIM technology in the AEC industry. This leads to the information management implications and the need to develop appropriate governance and security policies to maintain data quality and integrity ([18] #3).

Cybersecurity encompasses people, processes and governance issues, as well as their inter-relationships ([24] #4). It is critical for all actors operating and transacting within a Cloud-BIM implementation to understand the implications of cybersecurity ([19] #8). Under Cloud-BIM, the BIM development results in a broadening view that incorporates operating and transacting between people, governance, technology, and processes. Security policies are required to facilitate efficient BIM management in a Cloud platform throughout the construction project lifecycle, where vast amounts of data must be coordinated, exchanged, and protected in real time ([17] #4). Cloud-BIM requires the use of a secured framework that comprises confidentiality to access sensitive information, integrity for data assurance, validity, authenticity, and availability of data reliance and resilience. The study presents a Cybersecurity Management Framework for a Cloud-BIM computing model based on fundamental concepts, architectural principles, and challenges for implementation. The aim is to provide to the AEC research community a framework to incorporate a Cloud-BIM model into a project and to identify critical research directions in this new computing model paradigm ([21] #7). This contribution offers valuable insights to BIM practitioners involved in the development of Cloud-BIM integration, including the identification of cybersecurity threats and the management of distributed BIM data.

This study analyzes the implications of real and perceived threats that arise in a collaborative work environment. This study will aid the appropriate selection of Cloud technologies to benefit BIM integration.

The key questions addressed by this analysis are:

- What are the possible cyber-attacks on Cloud Computing?
- How can security risks, data loss, and other data related issues in BIM and Cloud integration be prevented?

An overview of Cloud Computing, the study of BIM, security threats, data breaches, data protection and the analysis of preventive measures are discussed in the following sections.

39.2 Related Studies

39.2.1 Building Information Modelling (BIM) Outline

Building Information Modeling (BIM) is a digital visualization of the functional and physical characteristics of a facility ([2] #44). BIM transforms the way in which we design buildings and manages the information about a facility forming a reliable basis for decisions during its life-cycle. BIM facilitates the interoperability exchange of data in digital format ([10] #8). It allows any aspect of a design's performance to be simulated and assessed before it is built. The virtual model becomes a reference for better construction. BIM offers more than just geometry, traditional building plans, elevations, sections were in the form of two-dimensions (2D) technical drawings and BIM extends the drawings to three-dimensions (3D), augmenting the primary spatial dimensions (width, height, and depth) with time as a fourth dimension (4D) and cost as a fifth dimension (5D) ([20] #7). It is an intelligent project model in which information about spatial relationships, geographic information, and properties of building components are embedded and shared between stakeholders throughout the process ([7] #122).

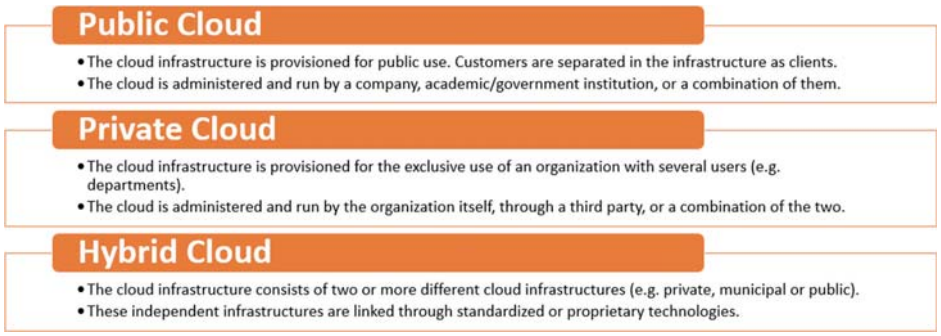

Fig. 39.1 Types of Cloud models

39.2.2 Overview of Cloud Computing

Cloud computing is a Web-based model for purchasing and provisioning IT services that include memory, storage, and complete applications. The main characteristics of Cloud computing are flexible, on-demand usage and the invoicing of IT services ([16] #6). Cloud computing delivers computing resources as services to end users by Cloud service providers (CSP). High-quality cloud services are provided by CSP to end users on request. Cloud computing is comprised of three layers: the system layer, the application layer, and the platform layer.

The system layer known as Infrastructure-as-a-service (IaaS) provides computational resources such as network devices, the infrastructure of servers, memory, and storage services as on-demand services [4]. This approach with the use of virtualization technology provides virtual machines that replace the physical equipment and eases a load of network administration as the clients are not required to monitor the health of the physical networks ([5] #30). The platform layer known as Platform-as-a-Service (PaaS) provides tools and libraries for application development where users can deploy and configure the settings ([4] #106). It provides a development platform for developers to design their specific applications, and hence developers are not required to purchase software development tools thereby reducing the cost ([9] #6). Finally, the application layer known as Software-as-a-Service (SaaS) is most commonly used by companies to reduce the cost of owning an application ([4] #106). Users can request applications from the CSP as per their requirements.

39.2.2.1 Various Types of Cloud Models

There are three different models of Cloud namely Public, Private and Hybrid. The Cloud model is selected based on the type of the data involved in the business, the level of security required, and the management desired ([12] #1). Figure 39.1 provides details about the various types of Cloud computing models.

39.3 Cloud-Based BIM Framework Development

The development of the framework is based on the analysis on security challenges involved in implementing BIM in the Cloud, directing a basic study concentrated on the following principal elements: (a) data breaches; (b) online cyber-theft; (c) cybersecurity attacks; (d) misuse of cloud computational resources. This analysis is followed by the development of the countermeasures that address the security challenges by implementing a prototype that provides a secure environment for BIM collaborators ([5] #9). The software development life cycle (SDLC) process is the underpinning methodology for the development of Cloud-based BIM platform. Model-View-Controllers (MVC) that consist of API, interfaces and governance strategies were chosen as the technical specifications for architecture development ([2] #1). Finally, the hosting Cloud environment was chosen for implementing the framework. The Amazon Web services(AWS) Cloud services was chosen as the hosting platform. The flow of the process of how the paper progresses to implement the Cloud-BIM framework is shown in is shown in Fig. 39.2.

Validation of the proposed Cybersecurity Cloud-BIM framework is through the implementation of countermeasure techniques for scenarios of possible cyber-attacks. Common cyber-attack scenarios include external and internal threat agents ([26] #1). An example of an external attack includes malicious outsiders who are not stakeholders in the construction project but who seek access to the BIM data for reconnaissance purposes. An example of internal attack is when stakeholders who are involved in the design, delivery, and operation of the project in some capacity abuse of their privilege of accessing BIM data by leaking sensitive information to the public ([23] #2). The framework also discusses research challenges in Cloud-BIM integration and the vision for this paradigm as it promises to change the use of information technology across the

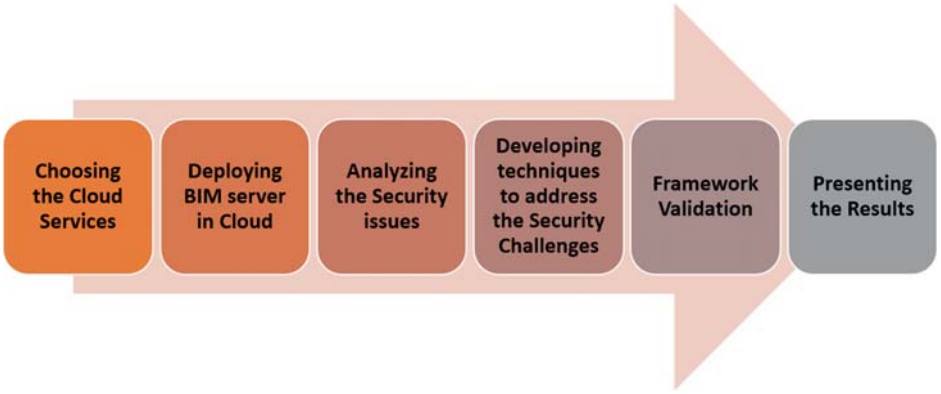

Fig. 39.2 Work flow of the framework development

construction industry ([8] #3). The following subsections discuss the analysis of the extensive study of security challenges in the Cloud environment and the countermeasure techniques that address the security challenges.

39.4 Prototype Implementation

39.4.1 Security Challenges in Cloud Computing

When using BIM in collaborative work environments, it is required to ensure information security and privacy. It is important to provide information access to the right people under the right circumstances ([5] #30). There are possibilities that collaborators may as well be competitors and have vested interests which lead to the stealing of the information. BIM, however, handles the access management in a single standalone system. It is important to maintain high access management standards in the collaborative platforms where multi-actors share common platforms ([14] #10). Lack of high standards, policies, and governance models leads to uncertainties and vulnerabilities as a result of the openness and highly decentralized nature in existence. Breaches may include loss of intellectual property, for instance, design or tendering related information ([7] #115). The BIM models have a proprietary governance approach and the governance policies must be compatible with the Cloud service provider.

The evolution of standardizations in Cloud computing is fragmented and hence it is difficult to define a unified approach that addresses the security, privacy, and governance of Cloud service providers. CSP's access management service requires advancements in privacy-reserving techniques. This includes maintaining the privacy agreements and implementing policies that suit the client's requirements. Maintaining poor standards and policies in virtualizations may lead to risks that include propensities to physical attacks, malware, viruses, and hacking ([22] #9). There also remains a general lack of understanding on the implication of data loss from BIM's perspective and the role of the CSP in data breaches. Perceptions of the increased risks are the biggest challenges in the process of integrating BIM and Cloud Technologies. As a result, project actors may be reluctant to adopt Cloud-based BIM for data sharing and exchange. In the following subsections, security threats in Cloud computing are explored from three perspectives: abuse use of Cloud computational resources, data breaches, and Cloud security attacks. The most common type of security challenges in Cloud computing is shown in Fig. 39.3.

39.4.2 Cloud-BIM Framework Architecture

The architecture of the Cloud-BIM framework is analogical to software architecture and is based on Cloud application architecture (SaaS) and Model View Controller (MVC) pattern. It consists of four main components: User Interface (UI), Cloud-BIM platform, Cloud Service Provider's infrastructure services and the countermeasure techniques represented in Fig. 39.4 ([2] #1).

Front End—User Interface (UI): The UI allows the user to perform necessary actions like insert, retrieve, edit, and delete on the BIM data. UI is a web page accessed via the web browser or a server over the Internet and is responsible for communication between Cloud-BIM and end-users ([2] #1).

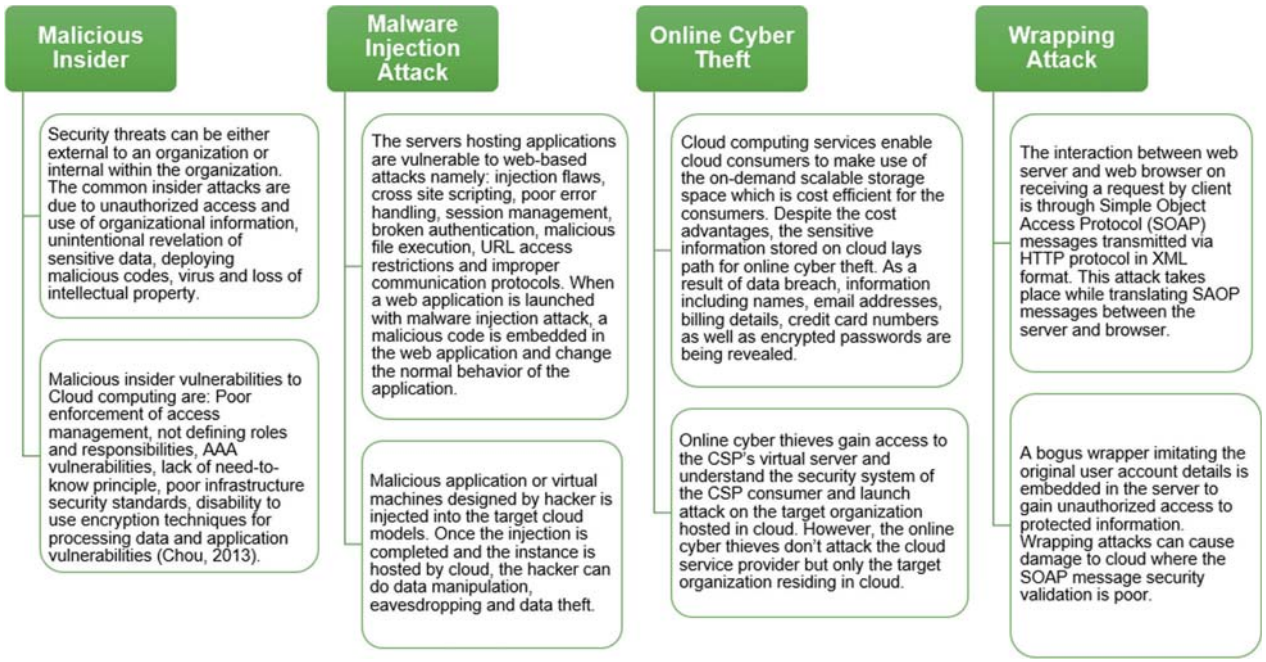

Fig. 39.3 Security challenges in Cloud computing

BIM Layer: The BIM framework layer plays a major role in the proposed architecture. It consists of three main parts:

- **BIM access API (Presentation Layer)**: This layer encompasses the View and Controller enabling end-users to access and use the framework services. The View represents the graphical representation of the Cloud-BIM model's back-end data ([3] #6). The Controller is responsible for the data flow between Cloud-BIM model and view. When the data in the model changes the view updates accordingly. Model and view are maintained separately by the controller ([2] #1).
- **BIM platform business and management logic (Application Layer)**: This layer comprises of the Model and is responsible for controlling different actions performed by end users. This represents the backend data of Cloud-BIM framework and contains the required logic to update the controller when the data changes ([2] #1).
- **BIM storage API (Database Layer)**: This layer is responsible for storing and retrieving Cloud-BIM data. This provides the mechanism to change the data to match the hosting environment i.e. Cloud service, database, and the underpinning technology with the help of DAO (Data Access Object) ([2] #1).

Hosting Cloud Service Provider and Infrastructure: This tier is managed by the CSP and provides the required infrastructure for hosting the Cloud-BIM project in Cloud ([16] #4). The CSP offers many services namely: security services, storage services, document handling, deployment services, communication services, and network services ([2] #1).

Countermeasures: The AEC industry is highly fragmented and has an exceptionally high perception of risk for Cloud computing because of the unique nature of the industry ([15] #123). In view of the Cloud-based BIM's multi-domain nature, there is the need for improving security and privacy management approaches for developing a secure collaborative platform. Solutions are multi-layered and can be categorized into infrastructure, agreement, information, and confidence ([24] #4). The suggested solutions span around technological, process and people issues. Secure, collaborative work environments with real-time data exchange are relatively novel within the AEC industry and require significant development. The requirements for a secure, collaborative Cloud-based BIM platform are reviewed in the following subsections. The most common countermeasure techniques fall under one of the areas namely (a) Access Management, (b) Governance approach, (c) Data Protection, (d) Secure Collaboration and (e) Security Policies ([15] #123).

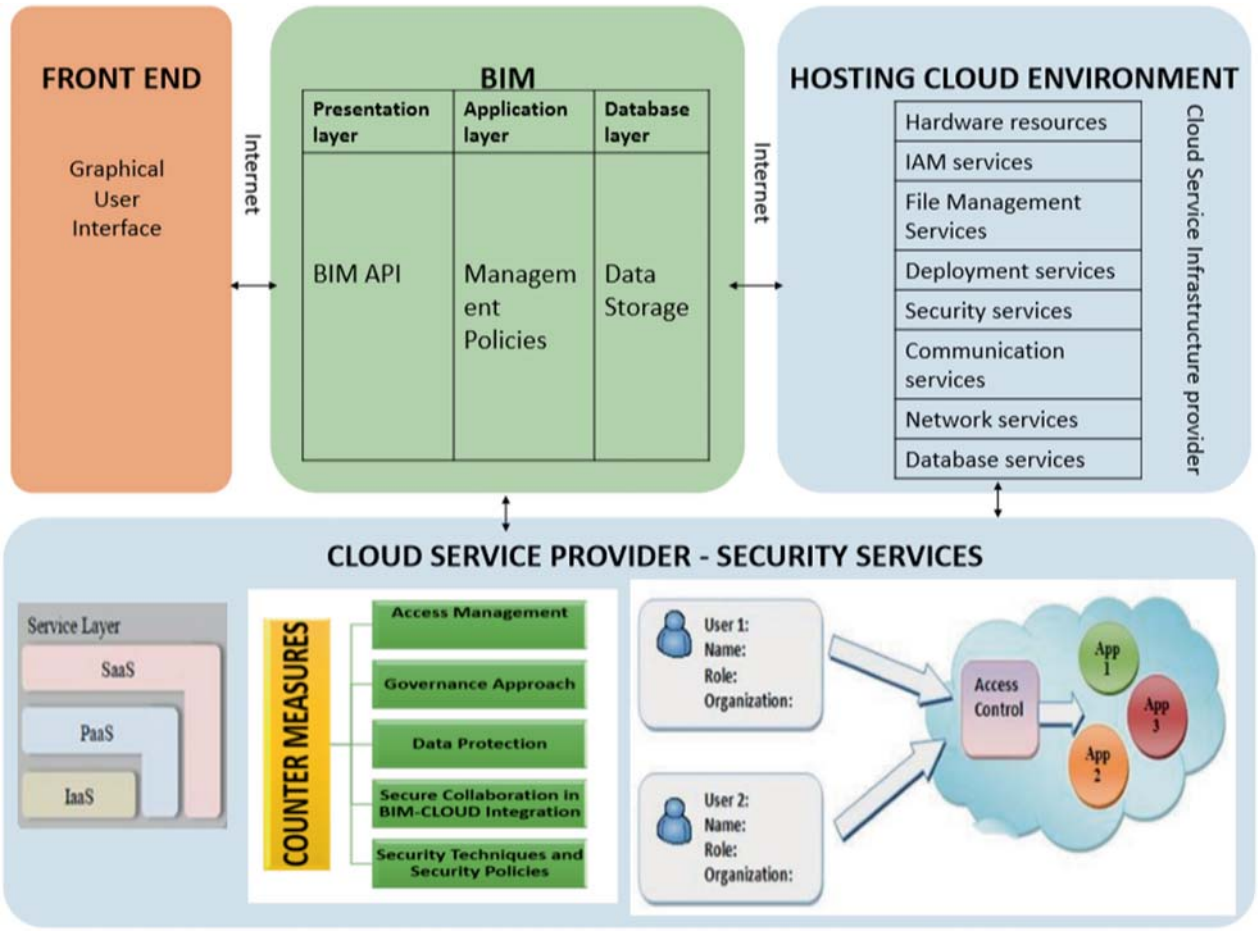

Fig. 39.4 Cloud-BIM framework architecture

39.5 Experimentation

The experimentation approach used for the prototype of Cloud-BIM framework is the simulation technique. The experimentation outcomes are demonstrations of the developed Cloud-BIM platform. The following concepts resulted in the demonstration of the developed Cloud-BIM platform prototype.

(a) **Access Management**

The user's access privileges consisting of authorization and authentication, which are key to the successful deployment of Cloud-based BIM for information exchange. It is required to combine role-based access privileges and visual quality such as Level of Detail (LOD) requirements together ([27] #2). BIM data stored in the Cloud is sensitive and private. The access control mechanisms, with the help of Identity Access Management, provided by CSP could be implemented to ensure that only authorized users may access the data. The continuous monitoring of data is required to ensure privacy in the physical computing systems where data is stored, especially with the increased use of mobile devices across geographically dispersed project environments where various stakeholders have access rights to shared data and models ([11] #120). Intrusion detection systems and configuring firewalls are common tools used to restrict unprivileged access and to monitor malicious activities ([6] #3).

When a user logs in as an administrator, the user is able to create roles for the actors, assign projects to the actors, create new project groups, assign domains, upload/remove BIM projects, track user activities, allow users to modify sensitive

information based on the requests received, define access rights to actors working from different locations, and assign stakeholder rights ([3] #6). Access rights assigned to BIM projects differ from one role to another. BIM objects are not completely removed from the database but are versioned and archived for future reference ([3] #6).

(b) **Data Protection**

Involving a third party in the collaborative BIM platform is common and the data can be accessed by multi-actors from multi-disciplines. Causes of data breaches by actors or by third-party users could be intentional or accidental. It is important to protect data from insider's threats as it is difficult to identify the insider's behavior. Security tools must be implemented to protect against insider threats ([1] #4). The security tools include: data loss prevention systems, authentication and authorization technologies, user behavior profiling, decoy technology, anomalous behavior pattern detection tools, and format preserving and encryption tools. These tools provide functions such as real-time detection for monitoring traffic, audit trails recordings for future forensics, and trapping malicious activity into decoy documents ([4] #106). Data can be classified based on the BIM data standards for masking, partitioning, and privacy protection to complement the access management policies. These must take into account, web-specific security challenges ([11] #118). Data protection techniques must be carefully tailored through standardization in order to not exacerbate interoperability across applications and infrastructure ([11] #118). Data partitioning and protection for a project in the AEC industry must be monitored through systematic risk assessment.

(c) **Governance Approach**

In collaborative work environments, it is recommended to use legal promises and guarantees in regulating relationships between collaborators to reduce the risks related to information usage. In the construction industry, relationships are mainly mediated through contracts and legal issues are critical when multi-actor communications are mediated by IT technologies ([13] #21). Regulation of information management must be drawn between the value of information sharing contractual types and the level of provisions. Lack of governance and data management in Cloud for contractual agreements and other legal issues might lead to a compromise of data integrity and privacy ([25] #2). The contractual issues and data ownership in shared web platforms are major barriers to the adoption of Cloud-based BIM environments. A governance approach addresses the contractual issues and provides clarity over data ownership. The governance approach establishes inter-organizational relationship management and develops trust, a critical attitudinal construct among the collaborators.

(d) **Security Techniques and Security Policies**

Implementation of security policies can reduce the risk of abusing Cloud technologies in collaborative work environments. Well established rules and regulations to terminate and isolate the spam or malware instances can help network administrators manage the Clouds more effectively. The malware injection attack is the major security concern in BIM Cloud integration. By implementing the File Allocation Table (FAT) system architecture, malware injection attacks can be prevented. The FAT table recognizes the instances consisting of the code well in advance. It compares the new instance with the previously executed instances in the customer's machine and validates the credibility of the new instance. Another way to prevent malware injection attacks is to store a hash value as an image file on the original service instance. The original and new service instances are compared to perform integrity checks and malicious instances are identified.

(e) **Secure Collaboration in BIM-CLOUD Integration**

The perceptions of risk and vulnerability slow down the process of adopting of BIM and Cloud technology in the AEC industry. In the AEC industry where large amounts of data are generated during a construction project, handling data including timeliness, completeness, or quality is critical. Data related risks are unacceptable and inconsistent with the goal of the AEC industry ([11] #120). To achieve secure, desirable, collaboration through BIM-Cloud integration, there is a need to address the risk issues as risk-related issues are the major inhibitors to achieving BIM Cloud Integration. A risk assessment framework, comprised of the following requirements, is postulated to establish a secure collaborative work environment:

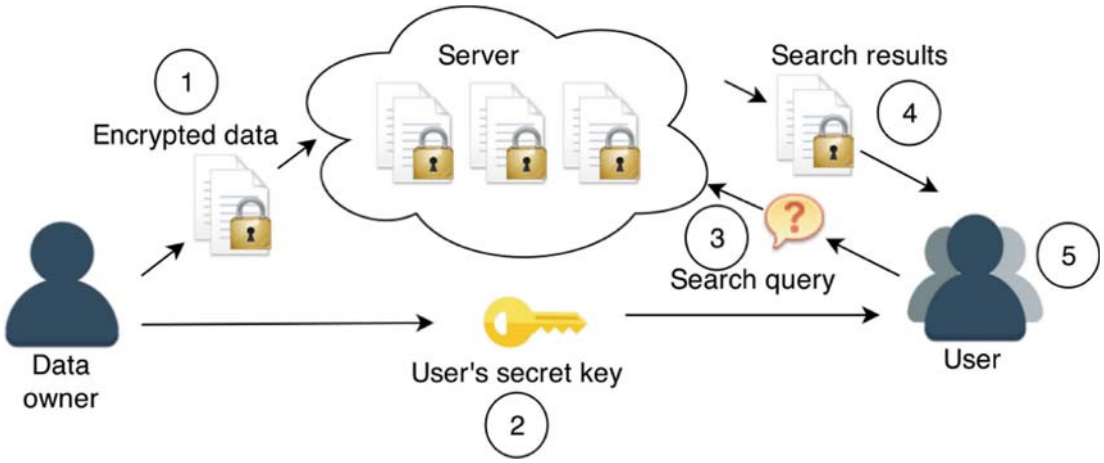

Fig. 39.5 Work flow in collaborative environment

- Secure BIM collaborative requirements are characterized by the cognizance of industry-specific needs: Infrastructure requirements, Technology requirements, Information Management and Data Governance, Contractual and Legal issues, and Relationship issues.
- Decisions on the selection of which IaaS, SaaS and PaaS options to adopt for the requirements of the construction project which meets the security standards during the data exchange and establishes interoperability throughout the lifecycle of the project.
- Cloud provider's security strengths based on technological and commercial factors must be incorporated into the client's policies to develop a stable governance model.

Secure Techniques for Collaboration Process: The project information varies depending on the domain. It is essential to adopt collaboration standards and have the administrator ensure that the common IFC standard is maintained throughout the project lifecycle ([2] #1). The standards are integrated automatically into the governance platform. Multi-actors practice this standard throughout the project lifecycle. The process and sharing of the secret key in a collaborative work environment are shown in Fig. 39.5.

39.6 Conclusion

There are many benefits of using Cloud computing such as cost efficiency, quick deployment, improved accessibility, etc. Despite the many advantages provided by Cloud computing for using BIM in a Cloud platform, the security challenges emanating from Cloud computing impinges the successful adoption of the Cloud-based BIM platform. Designing a secure, collaborative requirement for the BIM Cloud integration is a logical approach towards the development of the Cloud-based BIM platform for mitigating Cloud security risks. BIM-Cloud integration can be established successfully by tailoring Cloud technologies, according to the standards of the AEC industry, to bridge the gap between the AEC industry and the security risks in Cloud computing. An extensive study on the common security challenges faced in Cloud computing when integrated with BIM and their countermeasures is conducted and the results of implementing the framework with countermeasure techniques are presented in this paper.

Although our review has explored the field, further studies are needed to confirm the obtained results. Future work includes the extension of this review by including more sources (conferences, journals, and workshops) and questions. A future plan is to explore other security issues in the Cloud computing environment and we are also aiming to design an enhanced security model using encryption algorithms for data concealment in Cloud computing.

References

1. Alpcan, T., Başar, T.: Network Security—A Decision and Game-Theoretic Approach (2011)
2. Alreshidi, E., Mourshed, M., Rezgui, Y.: Cloud-based BIM governance platform requirements and specifications: software engineering approach using BPMN and UML. J. Comput. Civil Eng. **30**(4) (2016). https://doi.org/10.1061/(asce)cp.1943-5487.0000539
3. Beach, T., Rana, O., Rezgui, Y., Parashar, M.: Cloud Computing for the Architecture, Engineering & Construction Sector: Requirements, Prototype & Experience, vol. 2 (2013)
4. Chou, T.-S.: Security threats on cloud computing vulnerabilities. Int. J. Comput. Sci. Inf. Technol. **5**(3), 79–88 (2013). https://doi.org/10.5121/ijcsit.2013.5306
5. Das, M., Cheng, J.C.P., Kumar, S.S. Social BIMCloud: a distributed cloud-based BIM platform for object-based lifecycle information exchange. Vis. Eng. **3**(1) (2015). https://doi.org/10.1186/s40327-015-0022-6
6. El Mir, I., El Mehdi, K., Hanini, M., Haqiq, A., Kim, D.S.: A Game Theoretic Approach Based Virtual Machine Migration for Cloud Environment Security, vol. 9 (2017)
7. Gerrish, T., Ruikar, K., Cook, M., Johnson, M., Phillip, M.: Using BIM capabilities to improve existing building energy modelling practices. Eng. Constr. Architectural Manage. **24**(2), 190–208 (2017). https://doi.org/10.1108/ecam-11-2015-0181
8. Han, Y., Alpcan, T., Chan, J., Leckie, C., Rubinstein, B.: A Game Theoretical Approach to Defend Against Co-resident Attacks in Cloud Computing: Preventing Co-residence Using Semi-supervised Learning, vol. 11 (2015)
9. Hashizume, K., Rosado, D., Fernández-Medina, E., Fernández, E.: An Analysis of Security Issues for Cloud Computing, vol. 4 (2013)
10. Lu, Y., Wu, Z., Chang, R.-D., Li, Y.: Building Information Modeling (BIM) for green buildings: A critical review and future directions, vol. 83 (2017)
11. Mahamadu, A.M., Mahdjoubi, L., Booth, C.: Challenges to BIM-Cloud Integration: Implication of Security Issues on Secure Collaboration. Paper presented at the 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, 2–5 Dec. 2013
12. Mlotshwa, L., Leonard, A., Ntawanga, F.: A Conceptual Framework for Cloud-Computing Management: An End-User Environment Perspective. Paper presented at the 2015 IST-Africa Conference, 6–8 May 2015
13. Pauwels, P., Zhang, S., Lee, Y.-C.: Semantic web technologies in AEC industry: a literature overview. Autom. Constr. **73**, 145–165 (2017). https://doi.org/10.1016/j.autcon.2016.10.003
14. Rao, T., Haq, E.: Security Challenges Facing IoT Layers and its Protective Measures, vol. 179 (2018)
15. Redmond, A. M., Smith, B., Deke, M.: Environmental Performance of Buildings: Linking Practical BIM/ICT to Practical Policymaking (2014)
16. Rezgui, Y., Beach, T., Rana, O.: A governance approach for BIM management across lifecycle and supply chains using mixed-modes of information delivery. J. Civil Eng. Manage. **19**(2), 239–258 (2013). https://doi.org/10.3846/13923730.2012.760480
17. Salih, A.: A survey of Cloud Computing Security challenges and solutions, vol. 14 (2016)
18. Shen, Y., Li, K., Shi, W.: Advanced topics on cloud computing. J. Comput. Syst. Sci. **79**(8) (2013). https://doi.org/10.1016/j.jcss.2013.02.002
19. Shi, X., Jiang, H., He, L., Jin, H., Wang, C., Yu, B., Chen, X.: Developing an optimized application hosting framework in Clouds. J. Comput. Syst. Sci. **79**(8), 1214–1229 (2013). https://doi.org/10.1016/j.jcss.2013.02.003
20. Singh, V., Gu, N., Wang, X.: A theoretical framework of a BIM-based multi-disciplinary collaboration platform, vol. 20 (2011)
21. Soofi, A., Irfan Khan, M., Amin, F.-e.: A Review on Data Security in Cloud Computing, vol. 94 (2014)
22. Suryateja, P.: Threats and Vulnerabilities of Cloud Computing: A Review, vol. 6 (2018)
23. Tchernykh, A., Schwiegelshohn, U., Talbi, E.-g., Babenko, M.: Towards Understanding Uncertainty in Cloud Computing with risks of Confidentiality, Integrity, and Availability (2016)
24. Whitman, M., Mattord, H.: Principles of Information Security (2005)
25. Wong, J., Wang, X., Li, H., Chan, G.: A review of cloud-based BIM technology in the construction sector, vol. 19 (2014)
26. Yesilyurt, M., Yalman, Y.: New approach for ensuring cloud computing security: using data hiding methods, vol. 41 (2016)
27. Yu, S., Xiaolin, G., Jiancai, L., Xuejun, Z., Junfei, W.: Detecting VMs Co-residency in Cloud: Using Cache-based Side Channel Attacks, vol. 19 (2013)