applied sciences

MDPI

*Review*

# Cybersecurity Vulnerabilities in Off-Site Construction

**Kudakwashe Nyamuchiwa [1,*], Zhen Lei [2] and Clodualdo Aranas, Jr. [1]**

[1] Department of Mechanical Engineering, University of New Brunswick, Fredericton, NB E3B 5A3, Canada; clod.aranas@unb.ca
[2] Off-Site Construction Research Centre (OCRC), Department of Civil Engineering, University of New Brunswick, Fredericton, NB E3B 5A3, Canada; zhen.lei@unb.ca
* Correspondence: kuda.nyamuchiwa@unb.ca; Tel.: +1-506-429-8057

**Abstract:** Industry 4.0 is seeking to advance traditional construction practices towards more efficient and internet of things (IoT)-based construction practices, such as offsite construction. Offsite construction (OSC) allows for the simultaneous fabrication of building modules and onsite work. Integrating IoT technologies in construction practice is projected to improve the industry's growth. However, there is an increase in cybersecurity vulnerabilities. Cyber threats are becoming more disruptive and targeted, resulting in monetary and infrastructure losses. Furthermore, the COVID pandemic and the instability in Europe have seen over 100% increases in cyber-attacks, and most industries have weak cybersecurity protocols. The adoption of cybersecurity frameworks in the construction industry is sluggish, and the existing security frameworks fall short in addressing the needs of the industry. This paper gives a concise review of the offsite construction value chain vulnerabilities. We explore the existing cybersecurity frameworks and identify their limitations. Cybersecurity is presented as one of the most crucial components that has received little or no attention in OSC. The future of OSC is promising with the incorporation of Industry 4.0 technologies; however, its development needs to consider more proactive security approaches and management techniques that are adapted to the current hostile cyber landscape.

**Keywords:** cybersecurity; off-site construction; vulnerabilities



**Citation:** Nyamuchiwa, K.; Lei, Z.; Aranas, C., Jr. Cybersecurity Vulnerabilities in Off-Site Construction. *Appl. Sci.* **2022**, *12*, 5037. https://doi.org/10.3390/app12105037

Academic Editor: Giuseppe Lacidogna

Received: 23 April 2022
Accepted: 10 May 2022
Published: 16 May 2022



## 1. Introduction

Currently, production and manufacturing settings emphasize operational efficiency and sustainability, and the architectural, engineering, and construction (AECO) sectors are no exceptions. Industries, such as construction, have developed the coined term of "Construction 4.0", referring to the application of Industry 4.0 (IR4) to construction. Construction 4.0 incorporates a plethora of digital technologies in smart and cyber-physical systems [1]. These digital technologies come in the form of artificial intelligence (AI), additive manufacturing, big data, virtual reality (VR), blockchain, internet of things (IoT), big data, and other diverse forms depending on the area of application [2,3] (see Figure 1).

The impact of these technologies has been reported to improve productivity and efficiency through smart environments that are interconnected via the internet, creating diversified information sharing and storage, and management in the form of the internet of things (IoT). It is projected that, by 2025, the IoT will approach 950 billion in market size, a sign of its growth [3]. Based on studies by Zabidin et al. [4], the construction industry lags behind other domains, while other sectors, such as the manufacturing sector, have advanced further in digital technologies. Some of the barriers to adoption are the high initial costs through system modifications and the inevitable cybersecurity issues [5,6], which arise from the synergy of construction practice with digital technologies.

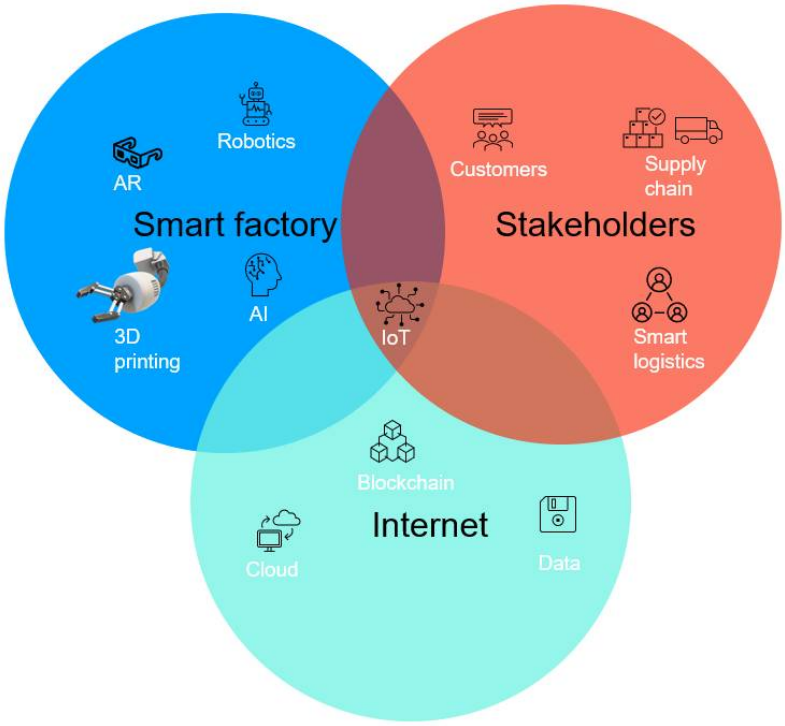


**Figure 1.** Multiple facets of Industry 4.0 and its integration in the IoT [1].

The digitalization of the construction industry has led to the extensive use of information and technological technologies (ICTs) throughout a project life cycle. As facilitated by the internet, this interconnectivity has created vulnerabilities that have created exploitable opportunities for malware breachers and cyber-attackers to preexisting systems in malicious attacks that use sophisticated tools to harvest unauthorized information and sabotage organizations [7]. On the other hand, the adoption of these technologies has been proven to shorten project durations, thereby, inevitably lowering project costs.

This interconnectivity has become the weakest link that counters the benefits of cyber-physical systems (Figure 1). A more focused approach to upgrading the current existing security frameworks and cybersecurity is thus necessary. Cybersecurity defines the instruments, strategies, and systems to secure data and additional hardware and human interaction [8]. Unfortunately, cyber-security implications and the related challenges have not received their due attention in proportion to the development of IR4 technologies in AECO.

As construction continues its upward trajectory toward digitalization, attacks are expected to rise, and security could potentially be the most significant setback towards fully adopting these digital technologies. Lessons can be drawn from well-established sectors, such as manufacturing, that are leading in digitalization. One of the emerging forms of construction is off-site construction (OSC), which simultaneously runs precast material manufacturing and onsite construction. Finished or semi-finished components are transported to the construction site for installation [9].

This merges two sectors, namely manufacturing and construction, creating a more complex system that requires specific and reliable cybersecurity infrastructure and organization. This paper addresses the importance of cybersecurity development in the off-site construction industry, highlighting the possible threats. Furthermore, we compare existing cybersecurity frameworks and the possibility of using blockchain technology as a management tool.

## 2. Cyber-Threats

### 2.1. Forms of Attack

As reliance on internet interconnected systems expands, proliferation risks also increase due to malicious software (malware). The most common forms of malware exist in the forms of viruses, worms, Trojan horses, and ransomware, and their effects on both individuals and organizations can cause financial strain, productivity disruption, and psychological distress. Malware functionality (payload) is often designed to steal sensitive information via remote access or disrupt systems and to demand a ransom. In addition, cybercriminals can create a network of compromised devices called bots that launch disruptive attacks. These are described in the next section.

#### 2.1.1. Viruses

The first recorded viruses were discovered in the 1980s and have grown exponentially in proportion to the expanding IoT systems [10,11]. This form of malware mimics its biological counterpart in that it requires a host to incubate and multiply, spread, and corrupt software and, in the worst-case scenarios, damage hardware [12–14]. During the advent of computers, viruses were contracted via infected removable devices, such as floppy disks. Currently, their vector spread is through malicious emails, browsing sites, and universal serial bus (USB) media. Viruses can disrupt system files, operate unwanted protocols, steal sensitive information, and damage operating systems.

#### 2.1.2. Worms

The worm form of malware, unlike a virus, does not require aided interaction, such as a host software, to infect other devices and is much preferred by cyber attackers [14]. Its mode of operation is based on self-operating and propagating software. Despite being autonomous, worms spread via network systems, peer-to-peer sharing networks (P2P), and electronic mail. As such, worms have a bearing on a system's much-needed processing performance. Such disruptions have resulted in system failures, as in the infamous case of the Morris worm, which had overreaching negative impacts on US national security. In terms of potency, worms are more effective than viruses because of their ability to affect several devices and programs in a system in a relatively shorter time compared with what viruses can achieve.

#### 2.1.3. Trojan Horse

The Trojan horse malware owes its name to the legendary tale of the deception at Troy by the Greeks. A significant number of illegal copyrighted works are infected Trojans. It masquerades as a legit application or program and, once admitted into a host system, it unleashes undesirable attacks that manipulate, damage, and destroy files. It is a non-duplicating form of malware; however, it overrides executable files with its malicious code. The original code will continue running while the malware gathers information from the system. Furthermore, this malware opens access to an attacker to steal information and remotely deny services to an entire network. Several organizations, including Microsoft, CNN, and Amazon, have been victims of such malware attacks [11].

#### 2.1.4. Spyware

Such malware can spy, monitor, and acquire information on remote devices. Information is stolen from individuals and organizations without them knowing it. Often, there is the remote activation of hardware, such as cameras and microphones and the stealing of sensitive information that may include design aspects or trade secrets of an organization.

### 2.2. Past and Present Threats

Malware was first introduced in the 1980s and has exponentially grown over the past decades [15]. Before the turn of the millennium, malware was perceived as a nuisance rather than a threat, and it has been argued that the damage caused by malware is over

magnified [16,17]. However, modern attacks are more calculated and profit-oriented with the development of increasingly integrated systems [3,18]. They are designed to cause distributed denial of service (DDoS), severe software and hardware damage, and even target other countries in addition to individuals and organizations. This is reflected in the estimated hourly losses of $US6500 by organizations [15].

From the early forms of malware, such as the Pakistani brain (1986), attacks have evolved to the more disruptive breaches, such as the Solarwind attack and Conti and Colonial Pipeline incidents [19,20]. The contributory effects of the COVID-19 pandemic and the instability in Europe have increased cyberspace usage [21–23]. Necessary changes need to be adopted to mitigate these threats in the construction industry. It is projected that, beyond 2022, there will be an expected increase in supply chain threats and attacks. Therefore, cyber protection measures must aim toward preventive solutions rather than mitigative. These include the need for real-time data transparency, early detection, swift responses, coordinated endpoint management, and awareness [24].

## 3. Importance of Cybersecurity in Manufacturing and Construction

Off-site construction is one of the emerging alternatives to traditional construction. The literature also refers to it as modular construction, prefab construction, prefinished volumetric construction, and precast construction [25,26]. These terms have a consensus of splitting the construction between a controlled manufacturing site and a construction site.

Construction and manufacturing have been categorized separately for decades with overlaps that show that they depend on each [27]; however, in retrospect, these two industries are not only reliant on each other but are part of the same value chain [28]. Currently, OSC is being implemented in individual unit and multi-family housing, commercial buildings, and the public service sector, such as hospitals and schools [28]. This sector is also adopting Industry 4.0 technologies, and it is projected to advance even further in the future [21].

The unique features of OSC involve transferring the construction elements to a controlled factory away from the construction site. This can potentially improve the safety and speed of construction and lower the waste production rates. It has been reported that OSC can potentially save between 30 to 50% of the project time due to minimized workforce movement [28]. Furthermore, a construction project on an estimated area between 10,000 to 20,000 $m^2$ can be delivered within 4 to 5 months [28].

Currently, the full potential of OSC is still futuristic. It remains limited in its adoption because of the extended supply chain that demands more coordinated monitoring between the manufacturing and construction parties. In addition, its adoption requires a restructuring of labor assignments and management, especially during the onsite assembly of the prefabricated modules. This inevitably requires critical skills, which counters the significant advantage of cost-savings given by OSC. The major cost-cutting benefit is drastically reduced to below 5% in total labor savings coupled with a steep learning curve [28].

However, for a fair assessment of the effectiveness of OSC over traditional construction, the period of this technology needs to be considered as well as other key performance indicators, which include the project payback period, return of investment, and labor cost [29]. As presented in this paper, the adoption of Industry 4.0 technologies must simultaneously be linked with cybersecurity upgrading and awareness, which is not currently practiced. Many organizations do not have the updated infrastructure to deal with the emergent vulnerabilities that provide room for cyber-attacks.

### 3.1. Manufacturing

Additive manufacturing is one of the emerging technologies adopted in OSC. The shortage of skilled labor in the construction industry partly contributes to its adoption as it minimizes the labor force required for operation [30]. Additive manufacturing allows the production of near-net-shape components based on a CAD system. It has been used to produce beam connections with enhanced stress-distribution properties.

As such, complexity and automation can be achieved by this technology with minimized raw material usage and time of operation, especially for components that require frequent repeatability [31]. Contrary studies indicate that utilizing this technology accrues costs higher than traditional construction because of unique functional property requirements in high-performance concrete [32]. The benefits of this technology relate to the added value to construction, which can be projected to cost savings over an extended period.

Additive manufacturing is a processing parameter-sensitive process, and a cyber-attack can result in remotely altering one condition, such as the raw material fill level and adjusting printing temperature [20]. These security breaches have more significant impacts than currently perceived, and they include the stealing of CAD/design files. This potentially leads to the unlawful production of components by an unauthorized party, which can ruin a company's reputation. Alternatively, a cyber-attack can alter printing parameters to introduce flaws in the printing.

In addition, a DOS can be issued until a ransom is paid. It is imperative to develop frameworks that can prevent, detect, and mitigate the undesirable effects of such attacks. Traditionally, manufacturing has been more concerned with blocking attacks on intellectual property. However, it is evident from the evolution of IoT in manufacturing and industry, which relies on cloud service and software, that the presented threats will be the most significant inhibitor in the future [33]. Cybersecurity concerns pose as weak links that threaten the survival of Industry 4.0 in construction.

According to Kebande [3], Incident Response Procedures (IRP) is one of the critical areas that have not been fully explored to the fullest potential. The Industry 4.0 concept in manufacturing, as in construction, seeks to improve its productivity and efficiency to by an estimated 15% to 20% [3]. As such, the high level of connectivity and internet dependence has resulted in an increase in the data volumes in the respective value chains in multiple uses [1]. These data exchanges can be seen in:

1. Processing of data for predictive maintenance and remote monitoring.
2. Enhancing service delivery and product quality.
3. Exchange of information among devices belonging to factories, contractors, and customers.
4. Mechanization and reduction of supplies.
5. Acquisition and storage of data for digital performance management.

As Industry 4.0 is currently promoting the application of its digital technologies resulting in complex connectivity, cybersecurity concerns are to take a mandatory approach in the setup stage rather than being a mere preference. As previously mentioned, the improvements brought by Industry 4.0 can prove futile because of the exponentially increasing security breaches [33,34]. According to Figure 2, the more the systems are integrated, the more malicious and subtle the security breaches can become.

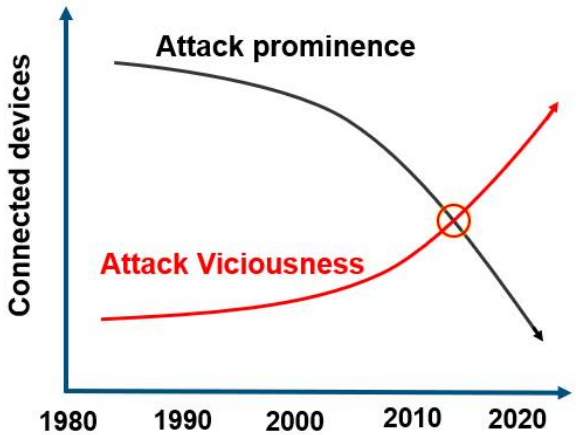


**Figure 2.** The growth and nature of attacks over the years [33].

### 3.2. Off-Site Construction

As previously alluded to, OSC combines the aspects of remote manufacturing and construction, enabling site work to progress with the prefabrication of building elements simultaneously. This is facilitated by multiple Industry 4.0 technologies, such as cloud services, sensors, GPS, and networks that involve the exchange of information in close to real time between different stakeholders, such as in BIM (building information management), which gives physical and functional digital reality to support the scheduling, design, building, operation, and upkeep of physical infrastructure, such as bridges and apartments [35].

One of the most extensively adopted technologies in OSC, more than any other digital technology, is BIM, which constitutes about 70% of 113 conducted research studies [26]. It has five main attributes (visualization, coordination, simulation, optimization, and plotting ability) that enable the digital simulation and modelling of a construction project during its entire lifecycle. This technology provides a pathway for the digitalization of OSC, and the key elements of this digitalization can be categorized as follows: digital data and access, automation, and connectivity.

In digital data and access, information is collected, processed, and analyzed to obtain new perspectives related to the value chain and giving information to be shared between stakeholders on a network. Stakeholders are enabled to operate electronic procurements and material accounts, leading to automation that engenders independent and self-ordering operations [27]. The installation of a 3D-printed parabolic exterior shaped wall module has been performed with precise dimensions being critical to fit the onsite assembly [31].

This work compares the accuracy of three formworks: a manual formwork, CNC formwork, and 3D-printed formwork, as depicted in Table 1.

**Table 1.** Comparison of manual, CNC, and 3D-printed formworks [31].

| Parameter | Manual Wood Formwork | CNC Formwork | Additively Manufactured Formwork |
|---|---|---|---|
| **Application** | All shell wall panels | All roof panels | Sample formwork of the shell wall panel |
| **Machine** | CNC cutting machine, woodworking tools | CNC cutting and milling machine | BAAM system, CNC milling machine |
| **Material** | Wood board, fiberboard, epoxy plaster | Rigid EPS foam, epoxy plaster | 20% carbon fiber with reinforced ABS polymer |
| **Accuracy** | Low | Low | High |
| **Production Cost** | Low | High | High |
| **Material waste** | High | High | Low |

In the manual formwork, the most significant deviation of 5.23 mm was observed at the points of maximum curvature. In terms of the dimensional accuracy, 3D-printed panels with CNC post-processing had a deviation of 1.29 mm and could sustain about 200 repeatable operations. Accuracy is an essential factor, and it is more critical during installation. Furthermore, secure information transfer and exchange become a greater priority since any falsification in the information can disrupt real-time information.

IoT in OSC has been used to perform supply chain supervision to track real-time work progression. Benefits have been realized regarding time savings, cost savings, and more efficient information sharing. However, studies have shown that the management of such complex systems experiences delays due to unstable networks and complex data handling [35].

This intrinsic weakness is an opportunist window for cyber-attacks that can compromise an already unstable system, which reflects the system's effectiveness [36]. A considerable investment is required to secure such a system. This often becomes the most

significant barrier to adopting Industry 4.0 in construction, given the compilation, securing, and processing of sensitive information on such systems [37]. The risk of a cyber-attack in OSC is augmented by the number of participants and extended value chains that involve stakeholders with limited security resources.

This also applies to contractors who might not be willing to spend many resources on securing their cyber systems [8]. The risk of a cyber breach can also be extended to the different project stages. This could be at the planning and design stages on the BIM, where vital information can be compromised or a DOS can be initiated, thereby, cascading into other project stages, such as construction, operation, and maintenance.

OSC is not only a clump of participants and equipment; with the adoption of IR4 technologies and digitalization of this industry, it has grown into a hyper-connected web of participants throughout an entire project life cycle. Hence, securing the cyber-physical interactions from the conceptual stages is paramount.

## 4. Targetable Entities and Vulnerabilities

To better understand the risks and vulnerabilities involved, this section explores the extensiveness of an OSC value chain that involves the design team, client, contractor, manufacturer, and third-party transportation crew and how their interactions are potential security breaches and vulnerabilities.

Vulnerabilities are security disparities that cyber attackers can manipulate. Therefore, an OSC value chain assessment is crucial for identifying potential weaknesses and possibly developing preventive and mitigative measures [38]. The process value chain for OSC can be split into Primary Production, Transportation, and Installation Production. An overview of a typical process is given in Figure 3.

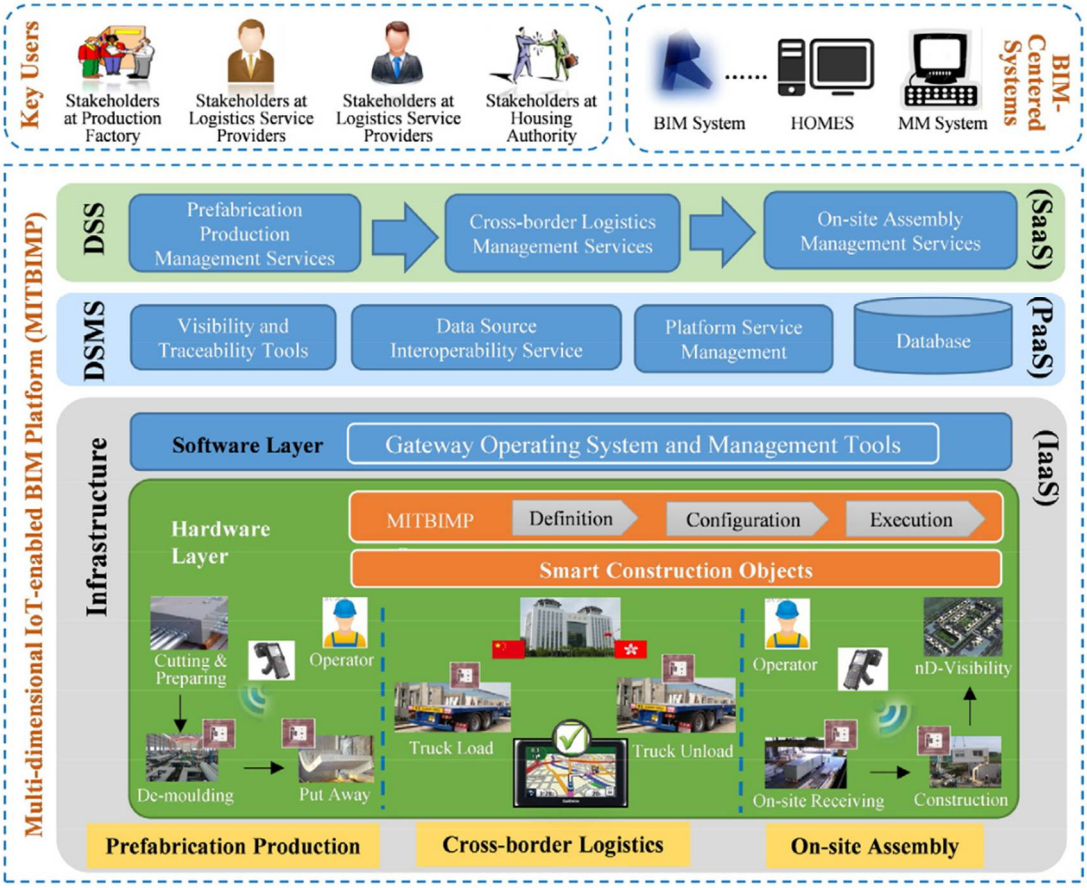


**Figure 3.** Offsite construction value chain. Reprinted with permission from Reference [35]. Copyright 2017 Copyright Elsevier B.V.

### *4.1. Primary Production*

In this stage, the following operations are performed.

#### 4.1.1. Prefabricated Module Production and Preparation

After the tender stage, the manufacturer and the onsite contractor communicate to deliberate the overall work plan. During this process, manufacturing drawings are prepared based on the initial design drawings, and these need to be approved by the onsite contractor before production is initiated. After approval of the production schedule, the production manager procures the necessary materials to produce prefabricated modules following the master plan and the project development [39]. An onsite agent of the factory traditionally facilitates communication between the factory and the site via email or fax to confirm custom orders.

Such traditional media has resulted in information loss and ineffective communication [35]. However, with digital technologies, such as multi-dimensional IoT building information modelling (MITBIMP) and radio frequency identification (RFID) devices, real-time information, such as the status of precast components can be effectively communicated [35]. This data sharing can also be enabled using smart construction objects (SCO) attached with auto-ID devices that are remotely located and gather information from remotely located value-adding points. Smart construction objects are enhanced by detecting, administering, computing, and responding.

The resulting autonomy and interaction with off-site work enable better decision-making [40]. A material list is prepared according to the work plan and ordered. Inspection samples are prepared and tested. A MITBIMP generates traceable data that gives information on the present and past statuses (see Figure 4). The cloud-hosted traceable data are based on the part history, which describes the previous location, handling, and processing history. Such a system overcomes the traditional problems of physical paper records that do not give real-time information and efficient information sharing without using emails or calls.


**Figure 4.** Visibility tools for MITBIMP. Reprinted/Adapted with permission from Reference [35]. Copyright 2017 Copyright Elsevier B.V.

Further integration has been enabled on MITBIMP systems by incorporating data source interoperability (DSIS) for smooth integration. This has been successfully implemented in Hong Kong, where an application information service (AIS) acts as a mediatory information system that can present heterogeneous information to stakeholders without human involvement. This service heavily relies on software, IoT, AI, and cloud services and is managed by an AIS Universal Description, Discovery, and Integration registry

(AIS—UDDI), facilitating cooperation amongst agents. With so much information being generated and requested, an SOA—based Data Access Services performs an information standardization sequence using a structured query language (SQL). This takes place under the following steps,

1. Retrieve data information model (DIM).
2. Target data source search.
3. Filter data.

Overall, the AIS agent retrieves the requested information and presents a data model representation [35].

#### 4.1.2. Transportation Design and Planning

Prefabrication logistics services have been used to monitor the entire logistics between the factory and construction sites. These use metaheuristic-based ant colony optimization (ACO) algorithms to give optimum pathways. ACO algorithms are a form of AI that is termed swarm intelligence. Artificial intelligence has also been vulnerable to adversarial forms of AI that can learn from other smart systems and generate noise to mask malicious activity to identify the computational limitations of another algorithm and possibly corrupt its training data [41].

The ultimate goal for transportation design and planning is to facilitate the timely delivery of prefab components, unlike in conventional systems where delays are experienced [39]. Once the precast components are completed, the swarm algorithm is invoked and linked to a BIM system. Optimized transportation models are generated as web-based features to allow end-user communication between the onsite crew and the factory. Real-time tracking has also been used (Kanban system [42]) to track the location and status of prefabricated components. The monitoring system uses RFID, and global positioning system (GPS) technologies for monitoring, and these are graphically presented to advise on the status, progress, and locations of the components [35].

#### 4.1.3. Onsite Assembly

Onsite assembly services are responsible for the administration, supervision, data handling, and real-time feedback at the prefabrication assembly points. Onsite, the administration is crucial for managing resources and onsite workers. Through RFID, each unit on the construction site can be identified, and site management is optimized to allocate resources where there are needed to shorten the assembly time.

Furthermore, this information is helpful for onsite safety management by identifying potential hazards and risks in advance. It has been reported that an 80% improvement can be achieved in emergency assessment [35,39]. Real-time tracking is also enabled to allow remote participants to know the project's progress. A model is shown in Figure 5 of real-time feedback implemented in a system that generates information for efficient supervision, control, and accurate decision-making from all involved parties [24].

Services, such as virtual reality (VR) presentation [43], have been used to relay real-time information regarding assembly status, labor assignments, and material utilization for concerted decision making. From the above-described value chain, it is clear that digital technologies are immensely beneficial as summarized in Table 2 [39].

Assessing the value chain of OSC, it is evident that cyber-physical interactions are necessary for accurate and real-time monitoring. In the OSC value chain, cyber-physical systems encompass a network of interconnected systems that can interact, monitor and control IoT-related devices with additional abilities to manipulate the physical environment [44]. Cyber-physical systems have a specific taxonomy comprised of three layers, and each layer is dependent on another [45]. The first layer, the perception layer, is responsible for interacting with the physical system and generating organized data based on its receiving feed.

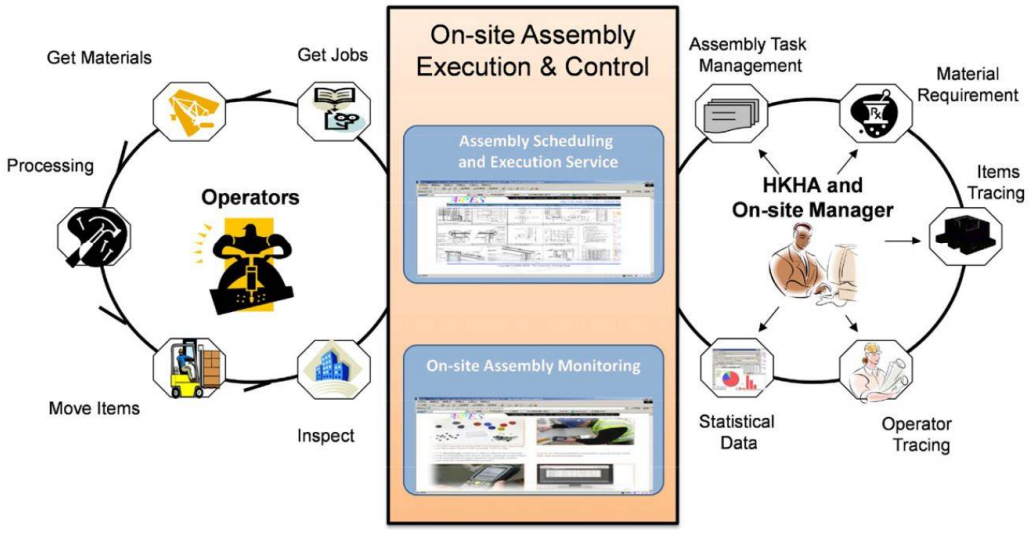


**Figure 5.** Execution and control during onsite installation. Reprinted with permission from Reference [35]. Copyright 2017 Copyright Elsevier B.V.

**Table 2.** Condition analysis of prefabricated module fabrication [39].

| Stages | KPI | Before | After | Improvement (+) |
|---|---|---|---|---|
| **Production** | Paperwork. | 10–20 papers | ≤9 papers | 10% |
| | Production Time. | 8–10 days | <7 days | 12.50% |
| | Emergency detecting. | 10–30 min | 3 min | 85% |
| | Emergency response. | 7 days | 0.5 days | 92.80% |
| **Transportation (time)** | Scheduling time | 1 day | 1–2 h | 66.70% |
| | Driver idle time | 5–10 min | 2–3 min | 66.70% |
| | Task realizing time | 5–10 min | 2–3 min | 66.70% |
| | Transportation time | 3–4 h | 2–3 h | 28.60% |
| **Assembly** | Emergency detecting time | 5 min | 1 min | 80% |
| | 4 day assembly cycle | 5–7 days | 4 days | 33.30% |
| | 6 day assembly cycle | 7–9 days | 6 days | 25% |
| | Emergency detecting time | 10 min | 2 min | 80% |
| | Module collection | 2 min | <1 min | 50% |

The perception layer comprises sensory devices and actuators, RFID tags, and GPS that collect real-time data, and secure control of these data is critical to secure feedback and control loops [38,46]. This layer can be identified in the previously discussed OSC value chain's primary production, transportation, and installation stages. Before analysis of information garnered in the perception layer, an intermediary layer, called the transmission layer, assists in exchanging and processing data obtained from the perception layer.

Cloud-computing services facilitate the transmission of data. Hence, it is crucial to secure the transmission before outsourcing the data to avert unwanted incursion and unauthorized access [47–49]. Finally, the transmitted information is passed into an executable command in the Application layer, which uses decision-making algorithms that allow automated design [41,50]. Data leaking is a possibility at this layer because of the handled volumes of data [41].

## 5. Cybersecurity Frameworks and Management

The benefits of IR4 technologies have great benefits to OSC. However, the previous section shows that network, auxiliary, and management vulnerabilities are inevitable along the supply chain. Different frameworks have been proposed to address these vulnerabilities. Some cybersecurity frameworks have been adopted into the construction sector based on

existing cybersecurity frameworks and standards. This section will explore some of the proposed frameworks and how they compare.

### 5.1. Cybersecurity Management Framework for Cloud-Based BIM Model

BIM use in shared work setups requires a secure means of passing information and privacy. Access to information should be granted to the right people at the right time. Hence, enacting security policies can reduce the risk of abusing cloud-based technologies in BIM. According to [51], malware injection is the primary threat to BIM cloud integration, and the proposed framework encompasses the management of data. As shown in Figure 6, information from the data owner to the final user does not take a direct route and requires special authorization. Protection of this information is thus crucial. The architecture of the framework consists of five levels of monitoring, which are

1. Access management.
2. Information protection.
3. Governance approach.
4. Security practices and policies.
5. Protected collaboration in BIM–cloud integration.

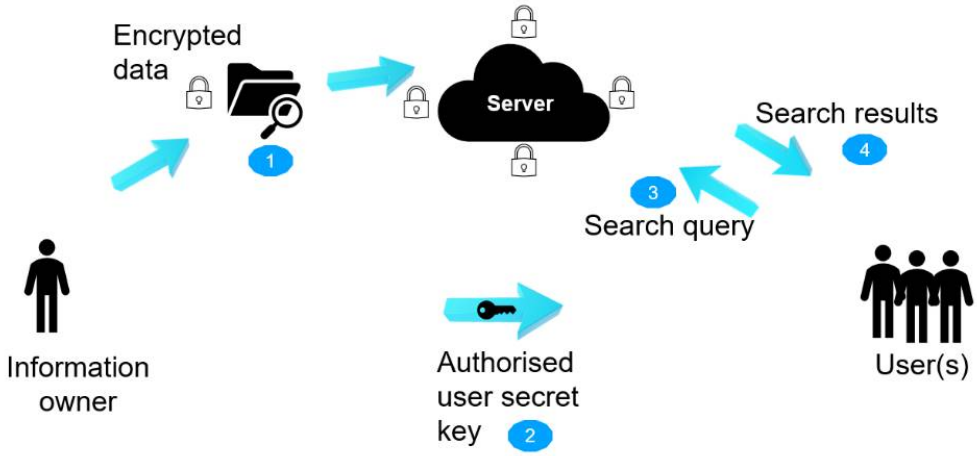


**Figure 6.** Data sharing with varied stakeholders [51].

#### 5.1.1. Access Management

Susceptible BIM information is stored in the cloud to enable restricted access. The control mechanism for access granting is the Identity Access Management system generated by the cloud service provider. This ensures that only authorized personnel have access to the information. Authorized users have the right to define roles for each member involved in the project allowing for the easy tracking of actions performed in the system.

The access rights assigned to each stakeholder are different based on their role in the project. In addition, data monitoring is enabled across different remotely located stakeholders to trace their access to the cloud-stored information [52]. Intrusion-detection systems and firewalls complement the data access to monitor any breaches. However, it is estimated that most data breaches involve stakeholders who intentionally or accidentally leak sensitive information. In most cases, stakeholders are involved in more than one project; hence, the roles overlap, which compromises the access to this information.

#### 5.1.2. Information Protection

Third-party involvement in collaborative OSC implementing BIM increases the risk of vulnerabilities. Regardless to say, they are necessary parties in the successful running of the project. Information needs to be protected from internal threats; however, this is done unintentionally in some cases. Data protection is achievable using multi-factor

authentication and authorization techniques, data loss prevention systems, the profiling of user behavior, detection tools for irregular behavior, and data encryption.

These techniques provide the real-time monitoring of data flow and exchange. According to BIM standards, information can be classified as relevant for masking, portioning, or privacy protection to complement access management. This information is stored for internal auditing and future forensic work to avoid aggravating information exchange across BIM–cloud platforms [53,54].

#### 5.1.3. Governance Approach

To secure information privacy between stakeholders, governance is necessary to regulate the collaboration and information sharing between the parties involved [55]. This makes use of verbal and written declarations and contracts that are legally binding. In the construction industry, relationships between stakeholders are facilitated through contracts. Regulation of such relationships is thus crucial when IoT technologies are involved. The regulation of data management must be established based on the value of the information and the level of access. The adoption of cloud-based services for construction faces a bottleneck due to the lack of clarity regarding data ownership. Proper governance can establish trust between stakeholders and inter-organizational solid relationships.

#### 5.1.4. Security Practices and Policies

The use of security policies can potentially reduce the risk of abusing cloud-integrated technologies in OSC. This can be achieved by passing well-formulated rules for administrators to stop and quarantine malware. Implementing a file allocation table (FAT) system reduces the risk of malware breaches. A FAT system can identify malware breaches during the execution of instances in advance. A credibility comparison is made between the previously run instance and the current one. Any discrepancies are highlighted, and the malware code is blocked [51].

#### 5.1.5. Protected Collaboration in BIM—Cloud Integration

To achieve protected collaboration in an integrated cloud system, matters concerning risk assessment are essential. Such initiatives give cognizance of the entire OSC value chain and provide a firm selection of the most favorable infrastructure as a service (Iaas), software as a service (SaaS), and platform as a service (PaaS) option that is relevant for a particular project. The cloud provider's claims based on technical and commercial factors must be merged into the client's policy formulation [51].

### *5.2. National Institute of Standards and Technology Framework*

The enactment of this framework is under the United States-based Cybersecurity Enhancement Act of 2014. Its focus is to provide good performance and cost-effective tactics to aid cyber-physical system stakeholders [56]. This ensures the reliable operation of critical infrastructure to minimize monetary and reputational risks.

The architecture of this framework is divided into three branches, namely: (1) The framework core—The core's key responsibility is to improve the communication of cybersecurity-related activities and outputs amongst different organizational levels covering management to implementation. (2) Tier implementation—the risks are assessed and managed based on the organization's code of conduct and workflow. (3) The framework profile—areas of improvement are identified, and the mismatch between the current modus operandi and the expected mode of operation is addressed [56]. An array of activities is defined to accomplish specific cybersecurity targets. The core can be divided into the following action points: Identify, Protect, Detect, and Respond.

**Identify**—The target is to bring an understanding of risk to a system that is vulnerable to cybersecurity breaches. Understanding the business context, resource allocation, and cybersecurity risks helps to focus and prioritize an organization's efforts in management

and strategies and operational needs. The expected outcome categories include: Asset supervision; Business setting; Governance; Risk evaluation; and Risk management policy.

**Protect**—This branch aims to create and apply suitable safeguards to guarantee the delivery of essential services and offers measures to support and mitigate the impacts of a potential cyber breach. The expected outcome categories include: Identity supervision and access management; Awareness and instruction; Information security; Data protection processes and procedures; Maintenance; and Defensive Technology.

**Detect**—Cybersecurity incidences are identified based on the implemented strategies. This allows for the timely discovery of security breaches. The expected outcome categories include Irregularities and incidents; Security constant monitoring; and Detection procedures.

**Respond**—The action response and containment of a cyber threat are the primary objectives. The expected outcome categories include Response Scheduling; Communications; Assessment; Mitigation; and Enhancements.

**Recover**—Appropriate activities are executed to restore any disrupted capabilities and services because of a breach. The expected outcome categories include Recovery planning; Improvements; and Communications. An overlap exists between the Response and Recover operations, thus, making it challenging to implement these measures.

The successful implementation of this framework helps to identify the existing and target cybersecurity conditions of a system, thereby, paving access to improvement and transparent communication between the stakeholders involved. This framework, as presented, has some limitations in that its implementation is biased toward critical infrastructure negating infrastructure, such as residential properties.

Furthermore, it lacks efficiency in cybersecurity risks in certain cyber-physical systems, such as BIM and MITBIMP involved in combined design, planning, and construction. One of the primary reasons for the sluggish adoption of IR4 in OSC is the lack of existing and fitting cybersecurity solutions. This proves problematic for the NIST framework to be implemented because its successful implementation is a preexisting system. Its primary focus is to reduce and improve management, which might not fully meet the significant concerns for OSC regarding identifying threats.

### *5.3. Security-Minded BIM in PAS 1192-5 and ISO 19650-5*

The PAS 1192-5 framework was established in May 2015 and was later withdrawn and replaced by the BN EN ISO 19650-5. However, it addressed the measures expected to form and cultivate appropriate safety and security attitudes and work culture across different stakeholders. This includes the need to observe and audit compliance. The approach applied in this framework was generalized for the most built asset or portfolio assets where data are created, stored, processed, and extracted in digital form. Its primary design was intended to support the development of cyber-physical systems.

However, it lacked a detailed taxonomy that could be followed in its implementation. The adoption of the ISO 19650-5 regarding security focuses on the secure management of sensitive information that is acquired, generated, handled, and saved as part of, or regarding, any other initiative, design, resource, product, or service. Its main components are based on the Parkerian hexad [57,58], which operates under confidentiality, integrity, availability, authenticity, possession, and utility.

This takes an extended form of the original CIA model [59]. The ISO 19650 series is applicable throughout the entire project or enterprise's lifespan and encourages the adoption of data management technologies [60]. Furthermore, its relevance in the built environment aims at how entities should guard their commercial data and intellectual property. Compliance with other legislation and standards exists, and these include the following (the list is not exhaustive):

1. Official Secrets Act 1989.
2. Computer Misuse Act 1990.
3. Data Protection Act 1998.
4. Environmental Information Regulation 2004.

5. Freedom of Information Act 2000.
6. Government Security Classifications.

As such, the functioning of this system is restricted to basic security for digital systems and typical information environments. In the case of OSC, which works on a combination of cyber and physical systems, a more broadened approach is expected rather than a mere access-based focus.

### *5.4. The Institute of Engineering Technology (IET) Code of Practice for Cybersecurity in the Built Environment (Cop-CSBE)*

The contents of this framework borrow from three pre-established security attributes, namely, the CIA model [59], the extended Parkerian hexad [58], and the Boyes model [61,62], including resilience and safety aspects. Under this framework, safety is defined as avoiding injury and harm to individuals, the workspace, and the associated operating equipment. An example related to this would be an intrusion into the removable dust system and processing parameters of an additive manufacturing machine resulting in the development of highly flammable material and overheating the equipment.

On the other hand, resilience improves a system's ability to transform, renew, and recover efficiently in the case of a cyber-attack. For an existing cyber-physical system, its resilience can be measured by how long it can endure the malfunction of communications and networking components before entire system failure [63]. This has been found to be critical for complex infrastructure where failure in one section is required to be isolated from the uncompromised zone.

To preserve data, cloud storage can be considered; however, if the attack simultaneously affects the connectivity of the infrastructure, very little can be done. The Cop-CSBE fails to clearly define the attributes of the Parkerian hexad and CIA security models. Elements of this framework are given in Table 3.

**Table 3.** Elements of the Cop-BCSE framework [64].

| Element | Understanding of . . . | Sample Questions |
| --- | --- | --- |
| People | Building system and human interaction (cause to effect). | Who requires access to system information? |
| Recognition and understanding. | Training and needs of participants involved in the project lifecycle. | What levels of cybersecurity needs are present? |
| Information and data. | Used information and data in the system. | What information and data are required for proper functioning of the system? |
| Electromagnetic spectrum. | Communication channels within and outside the system. | To what extent are communications confined within the system? Is remote access a requirement? |
| Building systems. | System location. | Is third-party access required? |
| Infrastructure. | Utilities supply (energy, telecommunication, water, and piping). | What physical and electronic infrastructure is used to generate, retrieve, handle, and store data, including network communication components? |
| Environmental factors. | Social, political, and legal factors relevant to the building and its system. | Should the information be analyzed, stored, and used within a single domain, or can it be accessed from another domain? |

### 5.5. Core Cybersecurity Framework for Construction

Building on the limitations of the Cop-BCSE framework of overlapping definitions and lack of full applicability in construction, Turk et al. [65] proposed the Core Cybersecurity, which is system- and process-based. Systems are defined as mechanisms that run processes that require security. A system aims to achieve a goal through the interconnectivity and interaction of different elements [66,67]. Construction can be seen as a conglomeration of different systems, and in the context of cybersecurity, every element of each system requires protection.

Alternatively, construction can be described as a process with corresponding inputs, outputs, controls, and resources. The resources manipulate the inputs to produce an output with the control mechanism guiding the process. The process can be broken down into subsequent processes, and securing every input, output, control, and resource is crucial for cybersecurity.

Unlike the extended Parkerian security structure with eight attributes that define cybersecurity as the presence of these attributes, the Core Cybersecurity framework is defined by the absence of wrongs. This counter approach is consolidated into three wrongs: stealing, lying, and harming [41]. Based on the extended Parkerian model, the attributes compare as shown in Table 4.

**Table 4.** Attributes of the Core Cybersecurity framework for construction [65].

| Extended Parkerian Attributes | Core Cybersecurity Model |
|---|---|
| Utility, availability, resilience, and safety. | Not harming. |
| Confidentiality and possession. | Not stealing. |
| Integrity and authenticity. | Not lying. |

The absence of these wrongs is considered for data, material, human resources, and systems, and they can be identified separately based on Tables 5–8.

**Table 5.** Forms of wrongs that can occur to elements [65].

| | Information | Material | People | System Mechanism | System Boundary |
|---|---|---|---|---|---|
| Stealing | Theft of information and assets. | Plain theft (indirect concern of cybersecurity). | Kidnapping (indirect concern of cybersecurity) | Plain theft. | Altering of system boundaries. |
| Lying | Fabricating or misrepresenting information. | Counterfeit and defective products. | Falsification of identity. | System claiming to be the authentic one. (Trojan horse) | System claiming to be the authentic one. (Trojan horse) |
| Harming | Corrupted information. | Physical damage to hardware and products (indirect concern of cybersecurity). | Hurting people (indirect concern of cybersecurity). | Altering the system by code or physically so that it malfunctions. | Creating loopholes on the boundary, disabling functionality. |

The specifics of this framework involve the unique nature of the construction industry, which often encompasses varied projects. In the case of OSC, the value chain is further complicated and requires security protocols at each value chain stage. The authors [65] presented a framework unique to construction that minimized the overlaps between attributes. Instead of labelled requirements, it presents the attributes as the absence of stealing, harming, and lying. This consolidates some of the overlapping attributes as presented in the Parkerian model.

**Table 6.** Vulnerabilities of construction data [65]. Reprinted/Adapted with permission from Reference [65]. Copyright 2021 Copyright Elsevier B.V.

| | **Stealing** | **Lying** | **Harming** |
|---|---|---|---|
| General construction information and databases. | Trespassing on intellectual property. | Falsifying information. | Withholding information. |
| Design information | Stealing reusable information and IP for other projects. | Deliberately sharing wrong information. | Destroying and eliminating information. |
| Bidding and costing information | Competitors attempting to obtain information on the level of pricing. | Deliberately sharing wrong information. | Destroying and eliminating information. |
| Construction information. | Accessing competitor trade secrets. | Deliberately sharing wrong information. | Destroying and eliminating information. |

**Table 7.** Wrongs towards stakeholders [65]. Reprinted/Adapted with permission from Reference [65]. Copyright 2021 Copyright Elsevier B.V.

| | **Stealing** | **Lying** | **Harming** |
|---|---|---|---|
| Authorities | Abduction. Identity theft. | Identity theft. Falsifying identity. | N/A |
| Knowledge staff (technocrats) | Abduction. Identity theft. | Identity theft. Falsifying identity. | N/A |
| Manual staff | N/A | Abduction. Identity theft. | Physical harm during interaction with machinery. |

**Table 8.** Wrongs that can happen to materials and resources [65]. Reprinted/Adapted with permission from Reference [65]. Copyright 2021 Copyright Elsevier B.V.

| | **Stealing** | **Lying** | **Harming Boundary** | **Harming Mechanism** |
|---|---|---|---|---|
| Legal person (operation, company, institution). | Change of ownership information. | Identity theft/ Falsifying identity. | Contravening boundaries to access insider information. | Disrupting internal processes. |
| Project virtual organization. | N/A | N/A | Contravening boundaries to access insider information. | Disrupting internal processes. |
| System softwares. | Pirating software. | Malware software that acts as a Trojan horse. | Uncontrolled access. | Disruption of the system by injection of malware. |
| OSC & construction site. | Stealing of design models. | Altering sensor data to give misleading information. | Uncontrolled site boundaries. | Operation of the value chain is disturbed by falsified information (software and hardware damage). |

The traditional cybersecurity approach simply secures the external system to protect the internal system. However, the implementation of IR4 technologies is greatly limited because of the strong overlapping as shown in Figure 7. Different stakeholders are involved in more than one project, and this model might not be best suited for the entire OSC value chain.

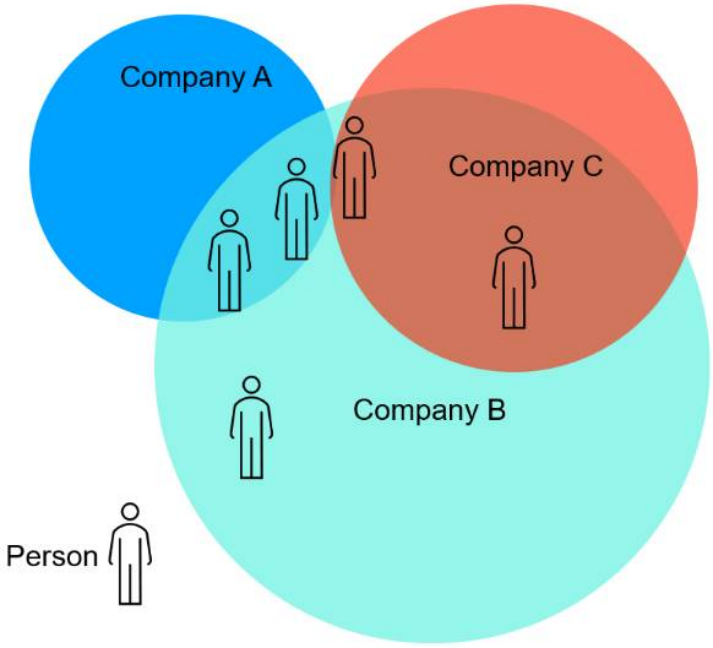


**Figure 7.** The overlapping nature of construction projects [65].

In assessing these frameworks, we find that all of them have similar principles that seek to attain the same goal. However, implementing these frameworks requires strategic management with digitalization and cybersecurity threats [9].

*5.6. Management*

As these technologies are adopted, there is an expected increase in research and development (R & D) investments [9]. However, a gap still exists in adopting management in IR4-enhanced construction. The gap is even wider for OSC, which trails behind the parent construction sector. With frequent information sharing through the entire life cycle of a construction project, information management tends to be a challenge that needs to be addressed [68]. The management of building information also involves managing legally important information that can be used in the event of disagreements and litigation amongst the stakeholders.

It has been suggested that the lack of security and protection protocols for digital property is one of the leading factors of poor management [69,70]. Surrounding these are legal factors that involve the ownership and right to access information. Blockchain technology is proposed to be a viable management tool. It works on the fundamental principle of chained information copied on multiple devices. Once chained, this information is secured and cannot be modified. Blockchain algorithms ensure that the copied data are identical to avoid conflicts [71].

Digital signatures play a crucial role in tracking the use of data across an entire network of users. Timestamps and author information can be monitored and provide an efficient way of managing complex systems. From a financial perspective, the overall costs of operating OSC operations can be minimized by using such algorithms to validate a block's proof of work [72]. The criterion for successfully using blockchain technology has been proposed [71] as shown in Figure 8. Not all operations will benefit from the use of blockchain. However, since complex overlaps exist between OSC stakeholders, they could benefit from its implementation.

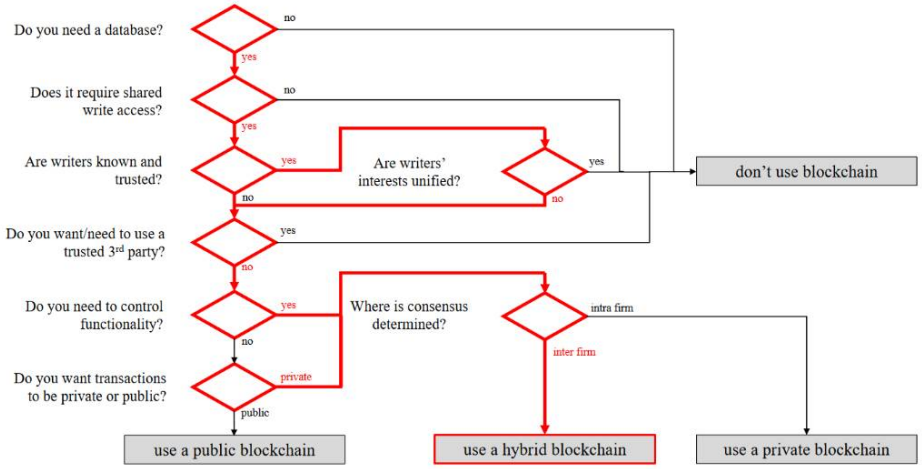


**Figure 8.** Blockchain user criterion. Reprinted/Adapted with permission from Reference [71]. Copyright 2017 Copyright Elsevier Ltd.

Management via blockchain can be achieved in four ways [71], and these are detailed as follows.

#### 5.6.1. Chained and Extremely Decentralized

Building data are transferred into a blockchain algorithm and copied across the network to the different participants. The files can be run from a plugin that monitors all version files (Figure 9).

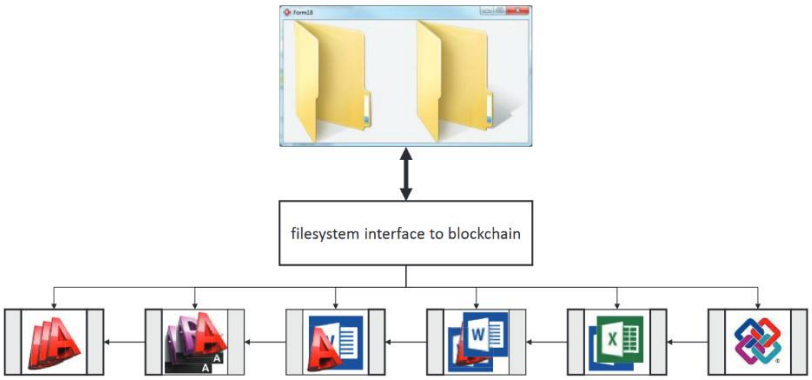


**Figure 9.** Chained and extremely decentralized management via blockchain. Reprinted/Adapted with permission from Reference [71]. Copyright 2017 Copyright Elsevier Ltd.

#### 5.6.2. Chained and Marginally Decentralized

Chained blockchains surpass the operating capacity of operating workstations because of the ever-increasing volumes of data. Information is pulled from the blockchain and is reserved locally when required to avert this problem. A minimum of one project partner must host the blockchain for other partners to gain access.

#### 5.6.3. Unchained

Data are not stored in the blockchain but traces and metadata are. Each stakeholder can trace the data's existence and is granted access to the files. The information can be integrated into the cloud or a file management server. This can be extended to a BIM setting that integrates a BIM server and the blockchain processor as shown in Figure 10.

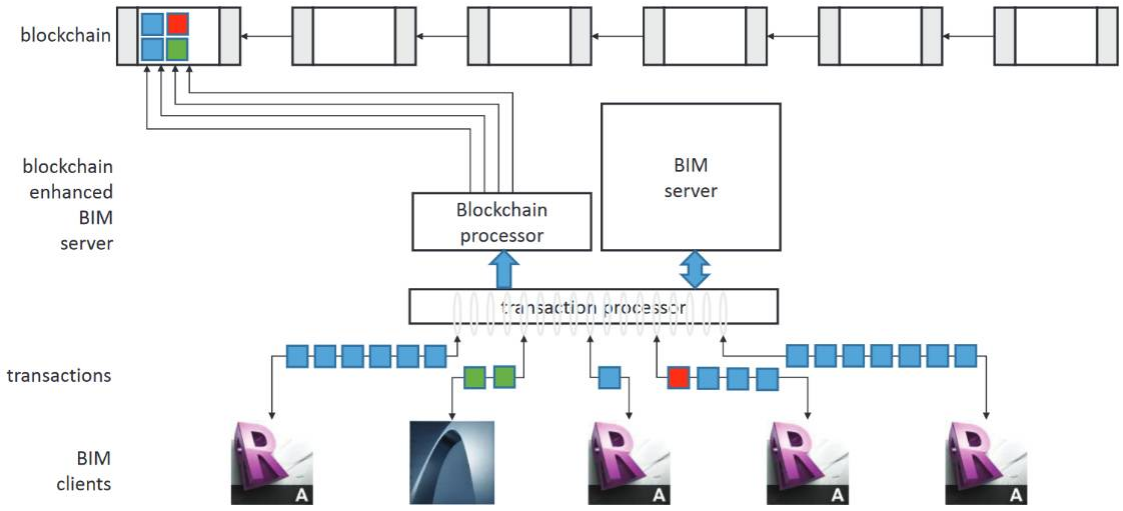


**Figure 10.** Taxonomy of blockchain management. Reprinted/Adapted with permission from Reference [71]. Copyright 2017 Copyright Elsevier Ltd.

As much as blockchain is a viable management tool, it lacks several aspects. The nature of blockchain technology requires a record of every transaction conducted by each network member. This is a costly redundancy that only serves the purpose of transparency and the elimination of intermediary roles [72]. In addition, the growth of a network causes scaling issues as many stakeholders are involved. The computational requirements and storage space are increased with network expansion. The issues of low performance and scalability increase the average time between creating new transactions and adding them to the existing blockchain [73].

Considering the issues of security, blockchain technology is reliant on the spending of processing power on the verification of operations and proof of work. The system's security is dependent on the central individuals responsible for the payment for the processing power. If many people are involved in managing the processing power of the blockchain network, it opens the possibility of security breaches [74]. Another issue arising that can make management difficult is privacy. Currently, blockchain solutions imply transaction verification from all users' block creation participation. This might not be well-suited for OSC since most of the information is considered sensitive and should be privy to the relevant personnel only [7,45].

## 6. The Future of OSC

Based on an analysis conducted by [26], the adoption of OSC is distributed mainly among nine countries, with China being the leading country in adoption. Such a low adoption of OSC is likely due to limited knowledge on implementing modular construction efficiently. In most practices, it is believed that poor and untimely implementation will result in the failure to achieve the projected targets [75].

An analysis is given in Table 9 with each country's publication's corresponding link strengths as well as the number of citations of the papers. The most significant contribution towards OSC implementation can be seen mainly in Asia with Mainland China having the most substantial contribution as represented by the most extended link in Figure 11 corresponding to a link strength of 3766. A more detailed breakdown is given in Table 9.

**Table 9.** Adoption of OSC initiatives based on the number of documents and citations in the top nine countries. The numbers indicate the number of citations per country [26].

| Country | Documents Published | Citations | Average Citation | Total Link Strength |
|---|---|---|---|---|
| Mainland China | 47 | 623 | 13.3 | 3766 |
| Canada | 18 | 93 | 5.2 | 4.94 |
| Hong Kong | 17 | 487 | 28.6 | 2250 |
| Australia | 15 | 81 | 5.4 | 1494 |
| USA | 15 | 99 | 6.6 | 616 |
| UK | 10 | 60 | 6 | 698 |
| Singapore | 8 | 101 | 12.6 | 1211 |
| Germany | 7 | 18 | 2.6 | 203 |
| Brazil | 6 | 34 | 5.7 | 240 |

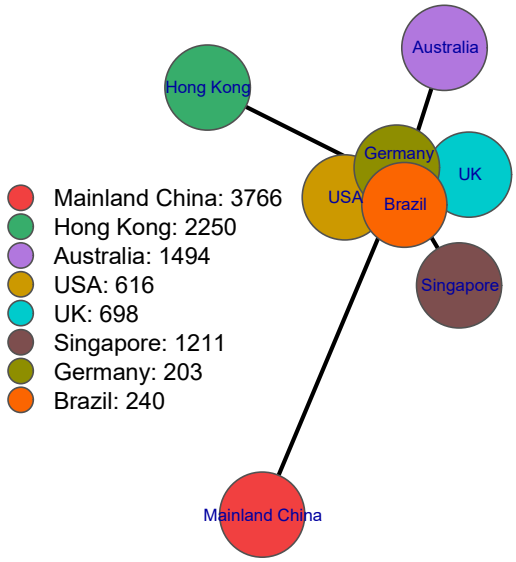


**Figure 11.** The dominance of OSC by country [26].

From these linkages, we observed that Canada and Hong Kong ranked second and third in terms of publications. However, Hong Kong has stronger links with other countries that is second only to China. This could be attributed to its proximity to China [76]. The future of OSC is dependent on the adoption of IR4 digital technologies. On the other hand, Canada's total link strength ranks it as number 7.

Based on a systematic review [26], about 13% of the publications discuss the implementation of digital technologies in the period between 2010 and 2020. Other than the top three leading countries, the United States, the UK, and Singapore show an active research influence on OSC, with BIM, IoT, RFID, and virtual reality being the most implemented technologies. The application of these digitalization technologies is expected to boost productivity.

However, the aspects of cybersecurity appear to not have efficient models adopted to the current security needs. With the COVID-19 pandemic and political instability in Europe, supply chains have been significantly disrupted [21]. This has spurred a rise in the cost of infrastructure and a greater shortage of housing. More efficient and innovative solutions have become a necessity, and unfortunately, traditional construction practices have seen decreasing profit margins due to inefficiencies. The pandemic has brought a new perspective regarding health and safety with physical distancing and a reduced work

force. These measures are not sustainable under traditional construction practices where everything is done onsite.

On the other hand, OSC factory and site settings can support such requirements because of their ability to decongest the work environment. In addition, an estimated 50% reduction in work-related accidents was reported for OSC activity [77]. With OSC comes improved productivity. An estimated 50% increase in productivity was reported for OSC [78]. Traditional construction has only seen an estimated 1% growth over the past two decades [79].

This has made traditional construction projects unpredictable due to uncertain timelines and costs. Standardized production has proven beneficial in the manufacturing sector because it enables a precise supply of materials reducing wastage, which is not the case in traditional construction practices. Despite the sustainable efforts to reduce wastage in traditional construction practices, an estimated 600 million tonnes of waste were generated in 2018 [80]. Such ongoing traditional practices will cease to be sustainable in the near future.

The future of OSC is indeed promising; however, as highlighted in this work, the vulnerabilities that these innovations face are worth considering. The political instabilities in Europe have changed how cyber threats are perceived because of increased cyber incidences [81]. A more proactive stance is required to protect data and infrastructure. Awareness has its limits, and the practical implementation of cybersecurity frameworks is paramount.

## 7. Conclusions

In this review, we presented the cyber vulnerabilities of adopting IR4 technologies in off-site construction. The reviewed literature noted that the OSC has experienced a sluggish adoption of IR4 due to increased costs, limited knowledge, and cybersecurity issues [5,6,25,26]. Cybersecurity was presented as one of the most crucial components that has received little or no attention in OSC based on the limited publications. For this purpose, this study was formulated to evaluate the malware risks associated with the digitalization of the OSC value chain and to perform an analysis on the existing cybersecurity frameworks.

In addition to the preliminary review of the cybersecurity vulnerabilities, threats, and risks of the OSC, this review can be used as a guide for presenting cybersecurity management in the complex OSC value chain, which encompasses IoT-based manufacturing and construction. After introducing the history of computer malware, we conducted a step-by-step analysis of the OSC value chain. We proposed that more emphasis is required at every stage of the construction and during the entire project life cycle process. A description of how an attack can be staged on an additive manufacturing OSC project was given.

The CIA framework was identified in the literature to be the most basic cybersecurity framework from which other frameworks branch, and it operates under confidentiality, integrity, and availability. Adding the modifications of utility, possession, and authenticity attributes establishes the Parkerian hexad. Further Boyes modifications resulted in the extended Parkerian hexad. These three cybersecurity models do not provide specifics to OSC, and, as modifications are made, they tend to take an incomprehensible complex form.

Moreover, the attributes they represent have substantial overlap with one another. For example, the definition of resilience in the extended Parkerian specifies how a system can endure the malfunction of communications and networking components before entire system failure [63], which has a similar meaning to the confidentiality attribute in the CIA model.

The NIST framework provides more simplified and distinct attributes but has extensively generic strategies. This approach is integrated with the ISO 19650-5 framework and has been applied in construction more effectively due to its simplified approach. Turk et al. [57] argued that frameworks should not be classified as wrong or right but as whether they are helpful or not. In principle, frameworks present what is expected for a secure cybersecurity system, and modifications are made as the scope and definition of expectations

expand. From the survey literature, there is no cybersecurity framework that has been tailored for the OSC industry.

We proposed the importance of adapted management, which incorporates blockchain technology despite limited attempts of its implementation in the construction industry. Blockchain technology was identified as a potentially secure way to ensure software and hardware security. The analysis conducted in this paper has made it clear that cybersecurity is more than simply a technical term.

The growth of the OSC industry depends on the development of competent and specific cybersecurity frameworks and management tools that meet the OSC sector's unique needs. We highlighted the significant risks and the currently available solutions that need to be improved to boost the growth of OSC. We recommend the development of an OSC-suited cybersecurity framework.

**Author Contributions:** Conceptualization, Z.L. and C.A.J.; methodology, K.N.; validation, K.N., C.A.J. and Z.L.; formal analysis, K.N.; investigation, K.N.; resources, Z.L. and C.A.J.; data curation, K.N.; writing—original draft preparation, K.N.; writing—review and editing, K.N., Z.L. and C.A.J.; supervision, C.A.J. and Z.L.; project administration, C.A.J. and Z.L.; funding acquisition, C.A.J. and Z.L. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by the Natural Sciences and Engineering Research Council of Canada (RGPIN-04126, RGPIN-04006).

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

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

## References

1. Mullet, V.; Sondi, P.; Ramat, E. A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0. *IEEE Access* **2021**, *9*, 23235–23263. [CrossRef]
2. Bai, C.; Dallasega, P.; Orzes, G.; Sarkis, J. Industry 4.0 technologies assessment: A sustainability perspective. *Int. J. Prod. Econ.* **2020**, *229*, 107776. [CrossRef]
3. Kebande, V.R. Industrial internet of things (IIoT) forensics: The forgotten concept in the race towards industry 4.0. *Forensic Sci. Int. Rep.* **2022**, *5*, 100257. [CrossRef]
4. Zabidin, N.S.; Belayutham, S.; Ibrahim, K.I. A bibliometric and scientometric mapping of Industry 4.0 in construction. *J. Inf. Technol. Constr.* **2020**, *25*, 287–307. [CrossRef]
5. Kozlovska, M.; Klosova, D.; Strukova, Z. Impact of Industry 4.0 Platform on the Formation of Construction 4.0 Concept: A Literature Review. *Sustainability* **2021**, *13*, 2683. [CrossRef]
6. Oesterreich, T.D.; Teuteberg, F. Understanding the implications of digitisation and automation in the context of Industry 4.0: A triangulation approach and elements of a research agenda for the construction industry. *Comput. Ind.* **2016**, *83*, 121–139. [CrossRef]
7. Ani, U.P.D.; He, H.; Tiwari, A. Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. *J. Cyber Secur. Technol.* **2016**, *1*, 32–74. [CrossRef]
8. Mantha, B.R.; de Soto, B.G. Cyber Security Challenges and Vulnerability Assessment in the Construction Industry. In Proceedings of the Creative Construction Conference, Budapest, Hungary, 29 June–2 July 2019. [CrossRef]
9. Maskuriy, R.; Selamat, A.; Maresova, P.; Krejcar, O. Olalekan Industry 4.0 for the Construction Industry: Review of Management Perspective. *Economies* **2019**, *7*, 68. [CrossRef]
10. Wójcicki, K.; Biegańska, M.; Paliwoda, B.; Górna, J. Internet of Things in Industry: Research Profiling, Application, Challenges and Opportunities—A Review. *Energies* **2022**, *15*, 1806. [CrossRef]
11. Hughes, L.A.; Delone, G.J. Viruses, Worms, and Trojan Horses: Serious Crimes, Nuisance, or Both? *Soc. Sci. Comput. Rev.* **2007**, *25*, 78–98. [CrossRef]
12. Senjo, S.R. *A Review Of "Robert W. Taylor, Tory J. Caeti, D. Kall Loper, Eric J. Fritsch, and John Liederbach, Digital Crime and Digital Terrorism"*; Studies in Conflict & Terrorism; Pearson/Prentice Hall: Upper Saddle River, NJ, USA, 2007; Volume 30, pp. 367–370, 397. [CrossRef]
13. Spencer, H.; Wang, W.; Sun, R.; Xue, M. Dissecting Malware in the Wild. In Proceedings of the Australasian Computer Science Week, Brisbane, Australia, 21 March 2022. [CrossRef]

14. Akinde, O.K.; Ilori, A.O.; Afolayan, A.O.; Adewuyi, O.B. Review of Computer Malware: Detection and Preventive Strategies. *Int. J. Comput. Sci. Inf. Secur. (IJCSIS)* **2021**, *19*, 49. [CrossRef]
15. Amin, M. A Survey of Financial Losses Due to Malware. In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, Udaipur, India, 4 March 2016. [CrossRef]
16. Hansen, R.L. The Computer Virus Eradication Act of 1989: The War against Computer Crime Continues Comment. *Softw. LJ* **1989**, *3*, 717–754.
17. Matkeviciene, R. Review: Cybercrime-Vandalising Information Society. Available online: http://informationr.net/ir/reviews/revs053.html (accessed on 29 March 2022).
18. Kamal, S.U.M.; Ali, R.J.A.; Alani, H.K.; Abdulmajed, E.S. Survey and brief history on malware in network security case study: Viruses, worms and bots. *ARPN J. Eng. Appl. Sci.* **2016**, *11*, 16.
19. Energy.gov, Colonial Pipeline Cyber Incident'. Available online: https://www.energy.gov/ceser/colonial-pipeline-cyber-incident (accessed on 8 April 2022).
20. Conti Ransomware | CISA'. Available online: https://www.cisa.gov/uscert/ncas/alerts/aa21-265a (accessed on 8 April 2022).
21. Machado, T.J.X.; Gouveia, L.B. Covid-19 effects on cybersecurity issues. *Int. J. Adv. Eng. Res. Sci.* **2021**, *8*, 222–229. [CrossRef]
22. Almeida, F.; Santos, J.D.; Monteiro, J.A. The Challenges and Opportunities in the Digitalization of Companies in a Post-COVID-19 World. *IEEE Eng. Manag. Rev.* **2020**, *48*, 97–103. [CrossRef]
23. War in Europe: Increased Cyber Security risk | Ek.co'. Available online: https://www.ek.co/gb/publications/war-europe-increased-cyber-security-risk (accessed on 22 April 2022).
24. CyberSecurity & Threat Intelligence Report 2021 | Heimdal', Heimdal Security Blog. 3 February. 2022. Available online: https://heimdalsecurity.com/blog/cybersecurity-threat-report/ (accessed on 29 March 2022).
25. Hwang, B.-G.; Shan, M.; Looi, K.-Y. Key constraints and mitigation strategies for prefabricated prefinished volumetric construction. *J. Clean. Prod.* **2018**, *183*, 183–193. [CrossRef]
26. Wang, M.; Wang, C.C.; Sepasgozar, S.; Zlatanova, S. A Systematic Review of Digital Technology Adoption in Off-Site Construction: Current Status and Future Direction towards Industry 4.0. *Buildings* **2020**, *10*, 204. [CrossRef]
27. Alaloul, W.S.; Liew, M.S.; Zawawi, N.A.W.A.; Mohammed, B.S. Industry Revolution IR 4.0: Future Opportunities and Challenges in Construction Industry. *MATEC Web Conf.* **2018**, *203*, 02010. [CrossRef]
28. Fenner, A.E.; Zoloedova, V.; Kibert, C.J. Conference Report 2017: State-of-the-Art of Modular Construction. In Proceedings of the Rinker School of Construction Management University of Florida, Gainesville, FL, USA, 28 October 2017. [CrossRef]
29. Woodhead, R.; Stephenson, P.; Morrey, D. Digital construction: From point solutions to IoT ecosystem. *Autom. Constr.* **2018**, *93*, 35–46. [CrossRef]
30. Pasco, J.; Lei, Z.; Aranas, C. Additive Manufacturing in Off-Site Construction: Review and Future Directions. *Buildings* **2022**, *12*, 53. [CrossRef]
31. Han, D.; Yin, H.; Qu, M.; Zhu, J.; Wickes, A. Technical Analysis and Comparison of Formwork-Making Methods for Customized Prefabricated Buildings: 3D Printing and Conventional Methods. *J. Archit. Eng.* **2020**, *26*, 04020001. [CrossRef]
32. Yang, H.; Chung, J.K.H.; Chen, Y.; Li, Y. The cost calculation method of construction 3D printing aligned with internet of things. *EURASIP J. Wirel. Commun. Netw.* **2018**, *2018*, 147. [CrossRef]
33. Wells, L.J.; Camelio, J.A.; Williams, C.; White, J. Cyber-physical security challenges in manufacturing systems. *Manuf. Lett.* **2014**, *2*, 74–77. [CrossRef]
34. Corallo, A.; Lazoi, M.; Lezzi, M.; Luperto, A. Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Comput. Ind.* **2022**, *137*, 103614. [CrossRef]
35. Zhong, R.Y.; Peng, Y.; Xue, F.; Fang, J.; Zou, W.; Luo, H.; Ng, S.T.; Lu, W.; Shen, G.Q.P.; Huang, G.Q. Prefabricated construction enabled by the Internet-of-Things. *Autom. Constr.* **2017**, *76*, 59–70. [CrossRef]
36. Fisk, D. Cyber security, building automation, and the intelligent building. *Intell. Build. Int.* **2012**, *4*, 169–181. [CrossRef]
37. Xu, G.; Li, M.; Chen, C.-H.; Wei, Y. Cloud asset-enabled integrated IoT platform for lean prefabricated construction. *Autom. Constr.* **2018**, *93*, 123–134. [CrossRef]
38. Yaacoub, J.-P.A.; Salman, O.; Noura, H.N.; Kaaniche, N.; Chehab, A.; Malli, M. Cyber-physical systems security: Limitations, issues and future trends. *Microprocess. Microsyst.* **2020**, *77*, 103201. [CrossRef]
39. Zhai, Y.; Chen, K.; Zhou, J.X.; Cao, J.; Lyu, Z.; Jin, X.; Shen, G.Q.; Lu, W.; Huang, G.Q. An Internet of Things-enabled BIM platform for modular integrated construction: A case study in Hong Kong. *Adv. Eng. Inform.* **2019**, *42*, 100997. [CrossRef]
40. Niu, Y.; Lu, W.; Chen, K.; Huang, G.G.; Anumba, C.J. Smart Construction Objects. *J. Comput. Civ. Eng.* **2016**, *30*, 04015070. [CrossRef]
41. Bécue, A.; Praça, I.; Gama, J. Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artif. Intell. Rev.* **2021**, *54*, 3849–3886. [CrossRef]
42. Junior, M.L.; Filho, M.G. Variations of the kanban system: Literature review and classification. *Int. J. Prod. Econ.* **2010**, *125*, 13–21. [CrossRef]
43. Wang, P.; Wu, P.; Wang, J.; Chi, H.-L.; Wang, X. A Critical Review of the Use of Virtual Reality in Construction Engineering Education and Training. *Int. J. Environ. Res. Public Health* **2018**, *15*, 1204. [CrossRef]

44. Gries, S.; Hesenius, M.; Gruhn, V. Cascading Data Corruption: About Dependencies in Cyber-Physical Systems: Poster. In Proceedings of the 11th ACM International Conference on Distributed and Event-based Systems, Barcelona, Spain, 19–23 June 2017; pp. 345–346. [CrossRef]
45. Chen, K.; Xu, G.; Xue, F.; Zhong, R.Y.; Liu, D.; Lu, W. A Physical Internet-enabled Building Information Modelling System for prefabricated construction. *Int. J. Comput. Integr. Manuf.* **2017**, *31*, 349–361. [CrossRef]
46. Khan, R.; Khan, S.U.; Zaheer, R.; Khan, S. Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. In Proceedings of the 2012 10th International Conference on Frontiers of Information Technology, Islamabad, Pakistan, 17–19 December 2012; pp. 257–260.
47. Hu, W.; Oberg, J.; Barrientos, J.; Mu, D.; Kastner, R. Expanding Gate Level Information Flow Tracking for Multilevel Security. *IEEE Embed. Syst. Lett.* **2013**, *5*, 25–28. [CrossRef]
48. Shi, L.; Krishnan, S.; Wen, S. Study Cybersecurity of Cyber Physical System in the Virtual Environment: A Survey and New Direction. In Proceedings of the Australasian Computer Science Week 2022, Brisbane, Australia, 14–18 February 2022; pp. 46–55. [CrossRef]
49. Sarfaraz, A.; Jha, A.; Mondal, A.; Goswami, R.T. *An Efficient Detection and Prevention Approach of Unknown Malicious Attack: A Novel Honeypot Approach*; Lecture Notes on Data Engineering and Communications Technologies; Springer: Singapore, 2021; Volume 73, pp. 11–19. [CrossRef]
50. Nagajayanthi, B. Decades of Internet of Things Towards Twenty-first Century: A Research-Based Introspective. *Wirel. Pers. Commun.* **2021**, *123*, 3661–3697. [CrossRef]
51. Mutis, I.; Paramashivam, A. Cybersecurity Management Framework for a Cloud-Based BIM Model. In *Advances in Informatics and Computing in Civil and Construction Engineering*; Springer: Cham, Switzerland, 2019; Volume 125, pp. 325–333.
52. Zhao, J. Design and Implementation of BIM Based Integrated Construction Management Platform in Cloud Environment. In *The International Conference on Cyber Security Intelligence and Analytics*; Springer: Cham, Switzerland, 2022; pp. 916–920. [CrossRef]
53. Mahamadu, A.M.; Mahdjoubi, L.; Booth, C. Challenges to bim-cloud integration: Implication of Security Issues on Secure Collaboration. In Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom, Bristol, UK, 2–5 December 2013; Volume 2, pp. 209–214. [CrossRef]
54. Ahmed, U.; Petri, I.; Rana, O.; Raza, I.; Hussain, S.A. Federating Cloud Systems for Collaborative Construction and Engineering. *IEEE Access* **2020**, *8*, 79908–79919. [CrossRef]
55. Wong, J.; Wang, X.; Chair, W.; Li, H.; Chan, G.; Li, H. A review of cloud-based bim technology in the construction sector. *J. Inf. Technol. Constr.* **2014**, *19*, 281–291.
56. *NIST CSWP 04162018*; Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018. [CrossRef]
57. Pender-Bey, G. *The Parkerian Hexad*; Information Security Program; Lewis University: Romeoville, IL, USA, 2019; p. 31.
58. Reid, R.C.; Gilbert, A.H. Using the Parkerian Hexad to Introduce Security in an Information Literacy Class. In Proceedings of the 2010 Information Security Curriculum Development Conference, Kennesaw, GA, USA, 1–3 October 2010; pp. 45–47. [CrossRef]
59. Carlson, T. *Information Security Management: Understanding ISO 17799*; Lucent Technologies World Services: New Providence, NJ, USA, 2001; p. 18.
60. Çekin, E.; Seyis, S. BIM Execution Plan based on BS EN ISO 19650-1 and BS EN ISO 19650-2 Standards. In Proceedings of the 6th International Project and Construction Management Conference (e-IPCMC2020), Istanbul, Turkey, 12–14 November 2020; p. 10.
61. Boyes, H. *Resilience and Cyber Security of Technology in the Built Environment*; Institution of Engineering and Technology: London, UK, 2013.
62. Boyes, H.; Hallaq, B.; Cunningham, J.; Watson, T. The industrial internet of things (IIoT): An analysis framework. *Comput. Ind.* **2018**, *101*, 1–12. [CrossRef]
63. Boyes, H. Security, Privacy, and the Built Environment. *IT Prof.* **2015**, *17*, 25–31. [CrossRef]
64. Boyes, H. *Code of Practice for Cyber Security in the Built Environment*; Institution of Engineering and Technology: London, UK, 2014.
65. Turk, Ž.; de Soto, B.G.; Mantha, B.R.; Maciel, A.; Georgescu, A. A systemic framework for addressing cybersecurity in construction. *Autom. Constr.* **2021**, *133*, 103988. [CrossRef]
66. Gammack, J.; Hobbs, V.J.; Pigott, D. *The Book of Informatics*; Thomson: Toronto, ON, Canada, 2007.
67. Tiwari, A.; Batra, U. Blockchain Enabled Reparations in Smart Buildings Cyber Physical System. *Def. Sci. J.* **2021**, *71*, 491–498. [CrossRef]
68. Turk, Ž. Ten questions concerning building information modelling. *Build. Environ.* **2016**, *107*, 274–284. [CrossRef]
69. Redmond, A.; Hore, A.; Alshawi, M.; West, R. Exploring how information exchanges can be enhanced through Cloud BIM. *Autom. Constr.* **2012**, *24*, 175–183. [CrossRef]
70. Thomas, L.W.; McDaniel, J.B. *Legal Issues Surrounding the Use of Digital Intellectual Property on Design and Construction Projects, No. 58*; National Academies Press: Washingdon, DC, USA, 2013.
71. Turk, Ž.; Klinc, R. Potentials of Blockchain Technology for Construction Management. *Procedia Eng.* **2017**, *196*, 638–645. [CrossRef]
72. Ammous, S. *Blockchain Technology: What Is It Good for?* SSRN Scholarly Paper ID 2832751; Social Science Research Network: Rochester, NY, USA, 2016. [CrossRef]

73. Chauhan, A.; Malviya, O.P.; Verma, M.; Mor, T.S. Blockchain and Scalability. In Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portuga, 16–20 July 2018; pp. 122–128. [CrossRef]
74. Kruglik, S.; Nazirkhanova, K.; Yanovich, Y. Challenges beyond blockchain: Scaling, oracles and privacy preserving. In Proceedings of the 2019 XVI International Symposium 'Problems of Redundancy in Information and Control Systems' (REDUNDANCY), Moscow, Russia, 21–25 October 2019; pp. 155–158. [CrossRef]
75. CII-Planning for the Future with Modularization and Offsite Construction'. Available online: https://www.construction-institute.org/blog/2021/september-2021/planning-for-the-future-with-modularization-and-of (accessed on 29 March 2022).
76. Xu, Z.; Wang, S.; Wang, E. Integration of BIM and Energy Consumption Modelling for Manufacturing Prefabricated Components: A Case Study in China. *Adv. Civ. Eng.* **2019**, *2019*, 1609523. [CrossRef]
77. How the Pandemic Will Shape the Future of Off-Site Residential Construction; Professional Builder. 2021. Available online: https://www.probuilder.com/how-pandemic-will-shape-future-offsite-residential-construction (accessed on 29 March 2022).
78. Stephenson, J. *Modular Building Institute-The Voice of Commercial Modular Construction*; Modular Building Institute: Charlottesville, VA, USA, 2021. Available online: https://www.modular.org/ (accessed on 29 March 2022).
79. Reinventing Construction through a Productivity Revolution | McKinsey. Available online: https://www.mckinsey.com/business-functions/operations/our-insights/reinventing-construction-through-a-productivity-revolution (accessed on 29 March 2022).
80. US EPA. Construction and Demolition Debris: Material-Specific Data. 12 September; 2017. Available online: https://www.epa.gov/facts-and-figures-about-materials-waste-and-recycling/construction-and-demolition-debris-material (accessed on 29 March 2022).
81. Djuraskovic, O. Cyber Attack Statistics. *50+ Important Facts and Trends'*; FirstSiteGuide. 2022. Available online: https://firstsiteguide.com/cyber-attack-stats/ (accessed on 29 March 2022).