Cybersecurity Vulnerabilities in Off-Site Construction

Subjects: Engineering, Civil

Contributor: Kudakwashe Nyamuchiwa, Zhen Lei, Clodualdo Aranas

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.

Keywords: cybersecurity ; off-site construction ; vulnerabilities

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**).

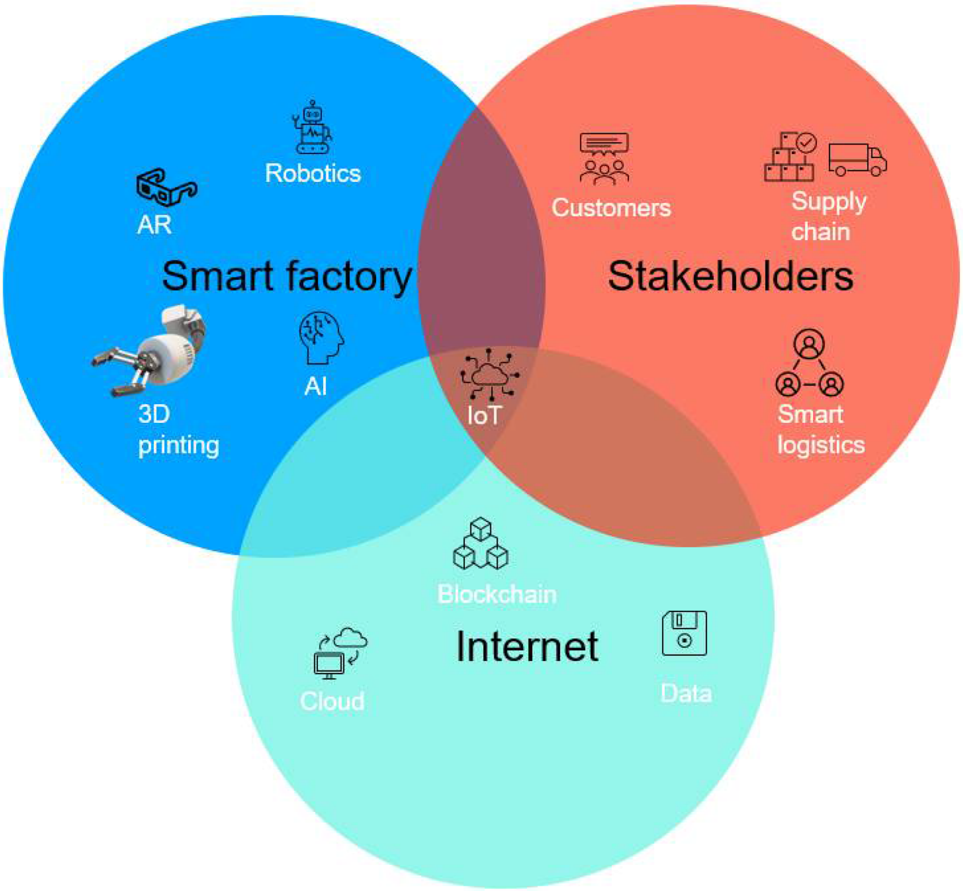

Figure 1. Multiple facets of Industry 4.0 and its integration in the IoT [1].

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.

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.

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.

2.2. Past and Present Threats

Malware was first introduced in the 1980s and has exponentially grown over the past decades [10]. 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 [11][12]. However, modern attacks are more calculated and profit-oriented with the development of increasingly integrated systems [3][13]. 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 [10].

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 [14][15]. 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 [16]; however, in retrospect, these two industries are not only reliant on each other but are part of the same value chain [17]. Currently, OSC is being implemented in individual unit and multi-family housing, commercial buildings, and the public service sector, such as hospitals and schools [17]. This sector is also adopting Industry 4.0 technologies, and it is projected to advance even further in the future [18].

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 [17]. Furthermore, a construction project on an estimated area between 10,000 to 20,000 m^2 can be delivered within 4 to 5 months [17].

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 [19]. 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.

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.

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 [21][22]. According to **Figure 2**, the more the systems are integrated, the more malicious and subtle the security breaches can become.

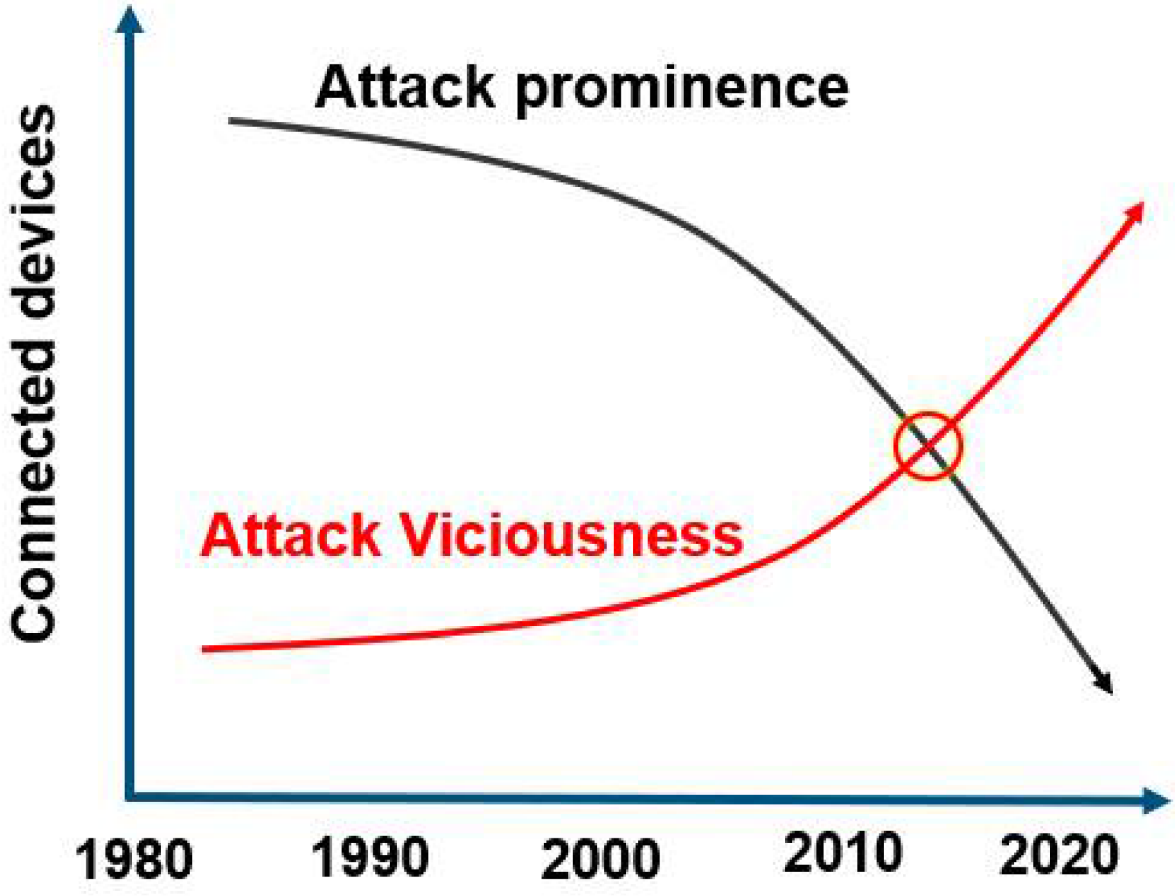

Figure 2. The growth and nature of attacks over the years [21].

3.2. Off-Site Construction

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.

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 [15]. 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 [16].

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 [23].

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

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 [24].

4.1. Primary Production

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 [25]. 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 [23]. 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 [23]. 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 [26]. 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. 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.

4.1.2. Transportation Design and Planning

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 [25]. 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 [27]) 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 [23].

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.

5. Cybersecurity Frameworks and Management

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 [28], malware injection is the primary threat to BIM cloud integration, and the proposed framework encompasses the management of data. As shown in **Figure 3**, 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

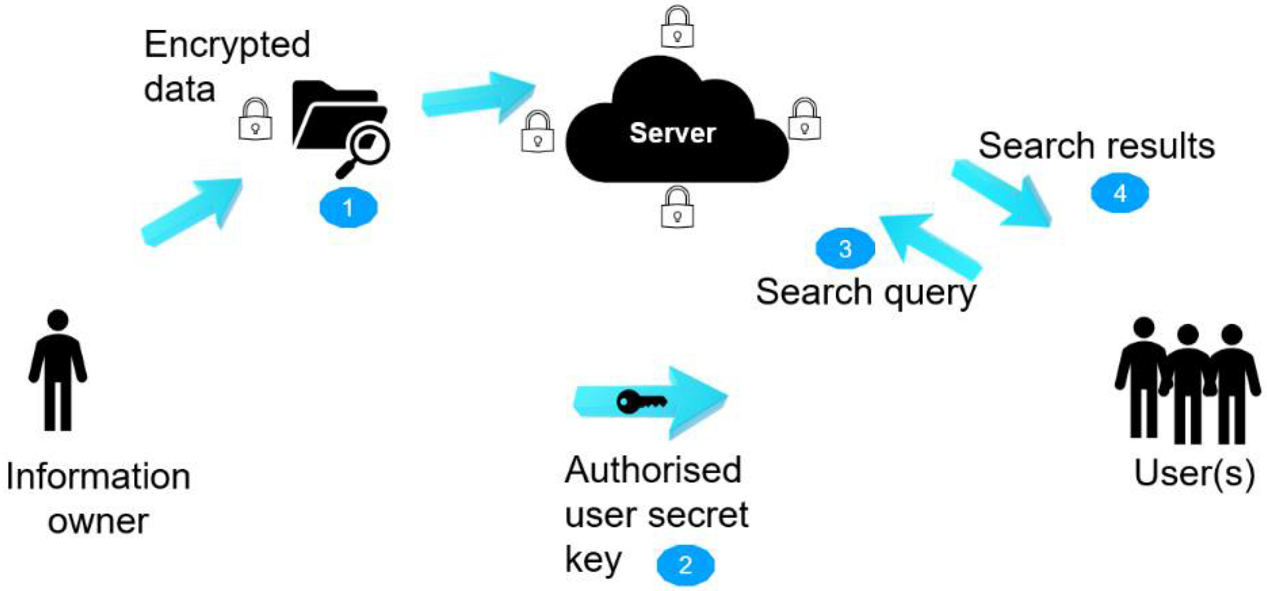

Figure 3. Data sharing with varied stakeholders [28].

- Access management.
- Information protection.
- Governance approach.
- Security practices and policies.
- Protected collaboration in BIM–cloud integration.

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 [29]. 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 [29]. 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.

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 [30][31], which operates under confidentiality, integrity, availability, authenticity, possession, and utility.

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 [32], the extended Parkerian hexad [31], and the Boyes model [33][34], 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 [35]. This has been found to be critical for complex infrastructure where failure in one section is required to be isolated from the uncompromised zone.

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. [36] 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 [37][38]. 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.

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 [39]. 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 [40][41]. 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 [42].

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 [43].

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.
2. Bai, C.; Dallasega, P.; Orzes, G.; Sarkis, J. Industry 4.0 technologies assessment: A sustainability perspective. Int. J. Prod. Econ. 2020, 229, 107776.
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.
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.
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.
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.
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.
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.
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.
10. 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.
11. Hansen, R.L. The Computer Virus Eradication Act of 1989: The War against Computer Crime Continues Comment. Softw. LJ 1989, 3, 717–754.
12. Matkeviciene, R. Review: Cybercrime-Vandalising Information Society. Available online: http://informationr.net/ir/reviews/revs053.html (accessed on 29 March 2022).
13. 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.
14. 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.

15. 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.

16. 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.

17. 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.

18. Machado, T.J.X.; Gouveia, L.B. Covid-19 effects on cybersecurity issues. Int. J. Adv. Eng. Res. Sci. 2021, 8, 222–229.

19. Pasco, J.; Lei, Z.; Aranas, C. Additive Manufacturing in Off-Site Construction: Review and Future Directions. Buildings 2022, 12, 53.

20. Conti Ransomware|CISA'. Available online: https://www.cisa.gov/uscert/ncas/alerts/aa21-265a (accessed on 8 April 2022).

21. Wells, L.J.; Camelio, J.A.; Williams, C.; White, J. Cyber-physical security challenges in manufacturing systems. Manuf. Lett. 2014, 2, 74–77.

22. 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.

23. 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.

24. 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.

25. 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.

26. Niu, Y.; Lu, W.; Chen, K.; Huang, G.G.; Anumba, C.J. Smart Construction Objects. J. Comput. Civ. Eng. 2016, 30, 04015070.

27. Junior, M.L.; Filho, M.G. Variations of the kanban system: Literature review and classification. Int. J. Prod. Econ. 2010, 125, 13–21.

28. 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.

29. NIST CSWP 04162018; Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018.

30. Pender-Bey, G. The Parkerian Hexad; Information Security Program; Lewis University: Romeoville, IL, USA, 2019; p. 31.

31. 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.

32. Carlson, T. Information Security Management: Understanding ISO 17799; Lucent Technologies World Services: New Providence, NJ, USA, 2001; p. 18.

33. Boyes, H. Resilience and Cyber Security of Technology in the Built Environment; Institution of Engineering and Technology: London, UK, 2013.

34. Boyes, H.; Hallaq, B.; Cunningham, J.; Watson, T. The industrial internet of things (IIoT): An analysis framework. Comput. Ind. 2018, 101, 1–12.

35. Boyes, H. Security, Privacy, and the Built Environment. IT Prof. 2015, 17, 25–31.

36. 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.

37. Gammack, J.; Hobbs, V.J.; Pigott, D. The Book of Informatics; Thomson: Toronto, ON, Canada, 2007.

38. Tiwari, A.; Batra, U. Blockchain Enabled Reparations in Smart Buildings Cyber Physical System. Def. Sci. J. 2021, 71, 491–498.

39. Turk, Ž. Ten questions concerning building information modelling. Build. Environ. 2016, 107, 274–284.

40. Redmond, A.; Hore, A.; Alshawi, M.; West, R. Exploring how information exchanges can be enhanced through Cloud BIM. Autom. Constr. 2012, 24, 175–183.

41. 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.

42. Turk, Ž.; Klinc, R. Potentials of Blockchain Technology for Construction Management. Procedia Eng. 2017, 196, 638–645.

43. Ammous, S. Blockchain Technology: What Is It Good for? SSRN Scholarly Paper ID 2832751; Social Science Research Network: Rochester, NY, USA, 2016.