Research Methods and Professional

Literature Review

Cybersecurity Threats in IoT in the Construction Industry

Table of contents

Introduction

The introduction of the Internet of Things (IoT) has brought about significant changes and innovations across multiple sectors, with the construction industry being one of the areas profoundly impacted by this ground-breaking technology (Kumar, Tiwari and Zymbler, 2019). IoT devices and systems are increasingly adopted in the construction sector to enhance productivity, safety, and efficiency (Woodhead et al., 2018). Smart sensors, wearables, and connected equipment facilitate real-time monitoring, data collection, and automation, which enhance decision-making and streamline processes (Tang et al., 2019; Rao and Lepech, 2021). However, the rapid integration of IoT within construction also introduces significant cybersecurity threats, potentially leading to financial losses, reputational damage, and compromised worker safety (Gheisari and Irizarry, 2016; Boyes et al., 2021). Despite increased awareness of these risks, comprehensive research addressing the specific cybersecurity challenges in construction is limited.

This literature review aims to fill this gap by analysing cybersecurity threats, challenges, and best practices specific to the construction industry's IoT adoption. The review seeks to answer the following research questions:

- What are the main cybersecurity threats faced by the construction industry in the context of IoT adoption?
- What are the technical, organizational, and regulatory barriers to achieving robust cybersecurity in construction IoT?
- What are the best practices and recommendations for mitigating cybersecurity risks in construction IoT?

The scope of this review encompasses an in-depth examination of existing literature on cybersecurity challenges in construction IoT, covering threats like unauthorized access, malware attacks, and insider threats, along with barriers to effective cybersecurity measures. Additionally, it discusses technical solutions, organizational measures, and policy recommendations to enhance cybersecurity. This synthesis of current knowledge aims to improve the understanding of cybersecurity in construction IoT

1. Background

1.1. Definition and concept of IoT in construction

The concept of the Internet of Things (IoT) in construction involves the integration of smart devices, sensors, and objects into various construction assets, machinery, and infrastructure to capture real-time data on location, performance, environmental conditions, and safety aspects (Silva dos Santos and Assayag, 2022; Katiyar et al., 2021; Dilakshan et al., 2021).

IoT in construction enables remote monitoring, predictive maintenance, enhanced safety, efficient resource utilization, and improved project management by transmitting collected data wirelessly to a central platform for analysis and actionable insights (Dilakshan et al., 2021; Silva dos Santos and Assayag, 2022; Maqbool et al., 2022). The application of IoT extents across different phases of construction projects, from design and planning to construction, operation, and maintenance (Dilakshan et al., 2021; Katiyar et al., 2021; Jiang and He, 2020).

1.2. Adoption and benefits of IoT in the construction industry

IoT is transforming the construction industry, driving efficiencies and improving safety and productivity. Mahmud, Assan, and Islam (2018) demonstrate that IoT technologies like BIM and smart sensors have reduced project timelines and improved productivity in Malaysia. IoT enables effective monitoring of equipment and infrastructure health, facilitating predictive maintenance and reducing operational costs (Burger, 2017; Censis, 2019).

Remote monitoring and control enhance worker safety by identifying potential hazards (Osunsanmi, Aigbavboa, & Oke, 2018). These advancements support Construction 4.0, integrating digital technologies for operational efficiencies, collaboration, and sustainability. As the industry embraces IoT, it will experience increased productivity, cost savings, and improved project outcomes.

1.3. Overview of cybersecurity in IoT

The integration of IoT has highlighted significant cybersecurity challenges due to the expanded attack surface. Butsianto et al. (2023) emphasize the need for robust encryption,

authentication, and intrusion detection to secure IoT networks. Jing et al. (2014) outlines layered security vulnerabilities, advocating for specialized strategies across awareness, network, and application layers. Ahmed et al. (2023) proposes lightweight cryptography and authentication mechanisms to address resource constraints in IoT devices. These papers underscore the importance of developing a holistic cybersecurity approach tailored to the unique aspects of the IoT environment, ensuring the integrity and confidentiality of interconnected systems and data.

2. Cybersecurity threats in construction IoT

2.1. Threat 1: Unauthorized access and data breaches

The threat of unauthorized access and data breaches in the Internet of Things (IoT) poses significant risks across multiple sectors. According to Hassija et al., (2019) unauthorized access can lead to severe disruptions. For example, in 2013, hackers stole the blueprints and building layouts of the Australian Intelligence Service headquarters, potentially compromising the security of the facility (Watson, 2018). In another incident, Turner Construction Co. suffered a data breach in 2016 that exposed tax information of many current and former employees (Sawyer and Rubenstone, 2019).

2.1.1. Relevant literature and findings:

The growing adoption of Building Information Modelling (BIM) and Internet of Things (IoT) in construction has increased the risk of unauthorized access and data breaches (Parn and Edwards, 2019). Cybersecurity vulnerabilities need to be assessed to protect sensitive information in the construction industry (Mantha and García de Soto, 2019). Turk et al. (2022) adapted the UK's National Cyber Security Centre framework to the construction context, highlighting the importance of governance, supply chain security, identity and access control, and data security in BIM/CDE environments. Tanga et al. (2022) emphasized that construction professionals must avoid cyber risks to protect project data and ensure satisfactory project delivery. Robust cybersecurity measures are crucial to mitigate risks associated with unauthorized access and data breaches in increasingly digitized construction environments.

2.2. Threat 2: Malware and ransomware attacks

The integration of Information Technology (IT) in construction operations has significantly increased vulnerability to cyber-attacks, notably malware and ransomware. For instance, the Sandworm group targeted German wind turbines in 2022 using malware, paralyzing 11GW of wind power capacity (Rekeraho et al., 2023). Ransomware attacks can disrupt construction operations, leading to project delays and financial losses. The Conti ransomware attack on a US federal construction contractor in 2021 resulted in data theft and encryption, impacting the company's operations (Tanga et al., 2022).

2.2.1. Relevant literature and findings:

Malware and ransomware pose significant threats to the construction industry. Viruses, worms, Trojans, and ransomware are common types of malwares that can infect construction systems, steal sensitive data, and disrupt operations (Tanga et al., 2022). Ransomware attacks can encrypt critical files and demand ransom payments, causing financial strain and project delays. Rekeraho et al. (2023) highlight the increasing vulnerability of IoT-based renewable energy systems to malware attacks. Mantha and Garcia de Soto (2019) emphasize the need for robust cybersecurity measures in the construction industry to mitigate the risks associated with malware and ransomware attacks. Adopting security best practices, employee training, and implementing advanced threat detection systems are crucial for protecting construction projects from these threats.

2.3. Insider threats and human errors

Mantha and Garcia de Soto (2019) briefly mentioned that most data breaches involve stakeholders who intentionally or accidentally leak sensitive information, posing a risk to construction projects. While not providing specific examples, this suggests that insider threats and human errors can compromise the security of construction data and systems. Alzubi et al. (2023) highlights that technological trust can be affected by various factors, including the perceptions of user usefulness and security. This implies that human factors play a role in the adoption and secure use of technologies in construction. Unintentional misuse or errors by insiders could undermine the security of cyber-physical systems. Tanga et al. (2022) note that

the construction workforce includes people from diverse socio-economic backgrounds with varying levels of cybersecurity knowledge and awareness. This diversity could contribute to an increased risk of insider threats and human errors if proper training and controls are not in place.

3. Challenges and barriers to cybersecurity in construction IoT

The construction industry faces significant challenges in adopting IoT and ensuring cybersecurity. Alshammari et al. (2021) note the absence of security in BIM standards and the need for a Building Automation System (BAS) that securely integrates IoT devices. Collusion and scalability issues emerge due to the complexity of blending IoT with traditional internet infrastructures (Kineber et al., 2023).

Organizational challenges stem from insufficient awareness and training among professionals. Onososen et al. (2023) point to low industry awareness and hurdles in recruiting qualified UAV pilots. Kineber et al. (2023) advocate for capacity building through educational initiatives like workshops and digital technology integration in programmes.

Regulatory and legal challenges involve data privacy, safety, and liability concerns. Alshammari et al. (2021) stress the importance of safeguarding data confidentiality, integrity, and availability. Onososen et al. (2023) address privacy, safety, and legal issues limiting Unmanned Aerial Vehicles (UAV) operations.

Recommendations include expanding BIM specifications for IoT compliance, enhancing standards for cybersecurity, and promoting government incentives to offset IoT adoption costs Alshammari et al. (2021). While, Kineber et al. (2023) suggest government interventions, such as credit facilities and incentives, to reduce the high initial capital investment required for IoT adoption and Onososen et al. (2023) proposed formulating clear policies and facilitating training to enhance competency.

4. Cybersecurity in construction IoT - Best practices and recommendations

To ensure cybersecurity in construction IoT, a multifaceted approach involving technical solutions, organizational measures, and policy recommendations is crucial. Encryption techniques like AES and 3DES can secure data transfer and prevent unauthorized access (Alshammari et al., 2021; Mantha and García de Soto, 2019). Advanced technologies such as Blockchain provide a decentralized and tamper-proof ledger for data storage and sharing (Kineber et al., 2023). Authentication measures, intrusion detection systems, firewalls, and honeypots are essential for preventing and mitigating cyberattacks (Turk et al., 2022; Alzubi et al., 2023; Rekeraho et al., 2023).

Organizational measures, including employee training, incident response plans, and continuous security evaluations, are vital for enhancing cybersecurity (Tanga et al., 2022; Sonkor & García de Soto, 2021; Mantha et al., 2021). Fostering a culture of embracing technological change and engaging third-party consultants can facilitate the adoption of secure IoT solutions (Kineber et al., 2023; Onososen et al., 2023).

Governments and industry bodies should develop specific cybersecurity standards and guidelines for the construction sector, considering its unique challenges (Mantha & García de Soto, 2019). Integrating cybersecurity concepts into existing data standards and establishing objective policies and regulations can address privacy and safety concerns (Alshammari et al., 2021; Onososen et al., 2023). Encouraging the sharing of best practices and lessons learned among construction companies can improve the industry's resilience to cyberattacks (Sonkor & García de Soto, 2021).

The literature emphasizes the importance of collaboration between academia, industry, and government to develop comprehensive cybersecurity frameworks tailored to the built environment (Alshammari et al., 2021). Key factors influencing the successful adoption of cyber technologies include knowledge, government support, culture, project nature, and regulations (Kineber et al., 2023).

5. Future research and directions

5.1. Gaps in current research:

Despite the increasing adoption of IoT in construction, research on cybersecurity threats and mitigation strategies specific to this domain remains limited. While studies have addressed IoT security challenges in general (Altulaihan, Almaiah and Aljughaiman, 2022), there is a lack of focus on the unique vulnerabilities arising from the deployment of IoT within the construction sector (Trotter et al., 2018). The majority of existing research concentrates on securing IoT devices and networks (Hadi, Alfoudi and Mahdi, 2022), with little attention given to the specific security requirements of construction IoT systems, such as protecting sensitive data, ensuring the integrity of connected equipment, and maintaining the safety of workers in the presence of IoT-enabled automation (Ahmed, Tahir and Lau, 2020).

5.2. Future directions

Future research should prioritize the development of comprehensive cybersecurity frameworks tailored to the construction industry, taking into account the distinct characteristics and challenges of IoT deployment in this sector. This could involve the creation of secure communication protocols, access control mechanisms, and data encryption techniques that are optimized for the resource-constrained devices and dynamic environments typical of construction sites (Trotter et al., 2018). Additionally, research should explore the integration of advanced anomaly detection and intrusion prevention systems that can effectively identify and mitigate cyber threats in real-time, considering the heterogeneous nature of construction IoT networks (Hadi, Alfoudi and Mahdi, 2022). Furthermore, studies should investigate the human factors associated with cybersecurity in construction IoT, such as user awareness, training, and observance to security best practices, to develop holistic approaches that address both technical and non-technical aspects of IoT security in this domain (Altulaihan, Almaiah and Aljughaiman, 2022).

Conclusion:

The literature review highlights the significant cybersecurity threats faced by the construction industry as it increasingly adopts Internet of Things (IoT) technologies.

Key findings: Key findings reveal that unauthorized access, data breaches, malware, ransomware attacks, insider threats, and human errors pose substantial risks to construction

IoT systems. The review also identifies technical, organizational, and regulatory challenges that hinder the implementation of robust cybersecurity measures in this sector.

Importance of addressing cybersecurity threats in construction IoT: Addressing cybersecurity threats in construction IoT is crucial to ensure the safety, reliability, and efficiency of smart construction processes. Failure to mitigate these risks can lead to severe consequences, including financial losses, project delays, reputational damage, and compromised worker safety. As the construction industry continues to embrace IoT, it is imperative that stakeholders collaborate to develop and implement comprehensive cybersecurity strategies tailored to the unique requirements of this domain.

Call for action and collaboration among stakeholders: This calls for action from construction companies, technology providers, researchers, and policymakers to work together in creating secure IoT solutions, establishing industry-specific cybersecurity standards, and promoting best practices. By fostering a culture of cybersecurity awareness, investing in employee training, and prioritizing the development of resilient IoT systems, the construction industry can unlock the full potential of IoT while safeguarding its digital assets and ensuring the security of its operations.

References:

Ahmed, A. A., Malebary, S. J., Ali, W., & Alzahrani, A. A. (2023). A Provable Secure Cybersecurity Mechanism Based on Combination of Lightweight Cryptography and Authentication for Internet of Things. Mathematics, 11(1), 220.

Ahmed, K.I., Tahir, M. and Lau, S.L., 2020. Trust Management for IoT Security: Taxonomy and Future Research Directions. In: 2020 IEEE Conference on Application, Information and Network Security (AINS). IEEE, pp.26-31.

Alshammari, K., Beach, T. and Rezgui, Y., 2021. Cybersecurity for digital twins in the built environment: current research and future directions. Journal of Information Technology in Construction (ITcon), 26, pp.159-173.

Altulaihan, E., Almaiah, M.A. and Aljughaiman, A., 2022. Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions. Electronics, 11(20), p.3330.

Alzubi, K.M., Alaloul, W.S. and Qureshi, A.H. (2023) 'Threats, Security and Safety of Cyber-Physical Systems in Construction Industry', in Advances in Cyber Physical Systems. Berlin: Springer.

Boyes, H., Isbell, R., Luck, A. and Moore, S., 2021. Security and privacy in the Internet of Things: Challenges and solutions for the construction industry. Automation in Construction, 124, p.103597.

Burger, R. (2017). How "The Internet of Things" is affecting the construction industry. The Balance Small Business.

Butsianto, S., Nugraha, U., Anwar, M., Anwar, S., & Judijanto, L. (2023). Cybersecurity in the Internet of Things (IoT) Era: Safeguarding Connected Systems and Data. Global International Journal of Innovative Research, 290-297.

Censis (2019). Getting started with IoT: Exploring IoT (Internet of Things) for business growth [Brochure], Glasgow: Censis.

Dilakshan, S., Rathnasinghe, A.P. and Seneviratne, L.D.I.P., 2021. Potential of internet of things (IOT) in the construction industry. In: Sandanayake, Y.G., Gunatilake, S. and Waidyasekara, K.G.A.S. (eds). Proceedings of the 9th World Construction Symposium, 9-10 July 2021, Sri Lanka. [Online]. pp. 445-457. DOI: https://doi.org/10.31705/WCS.2021.39.

Gheisari, M. and Irizarry, J., 2016. Investigating human and technological requirements for successful implementation of a BIM-based mobile augmented reality environment in facility management practices. Facilities, 34(1/2), pp.69-84. https://doi.org/10.1108/F-04-2014-0040

Hadi, Q.A., Alfoudi, A.S. and Mahdi, A.M., 2022. IoT Cybersecurity Threats and Detection Mechanisms: A Review. Wasit Journal for Pure Sciences, 2(2), pp.231-250.

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., Sikdar, B. (2019). A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. IEEE Access 7 : 82721-82743. ScholarBank@NUS Repository.

Jiang, Y., and He, X., 2020. Overview of Applications of the Sensor Technologies for Construction Machinery. IEEE Access, 8, 110324–110335. doi: 10.1109/ACCESS.2020.3001968

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. Wireless Networks, 20(8), 2481-2501.

Katiyar, A., Kumar, P., 2021. A Review of Internet of Things (IoT) in Construction Industry: Building a Better Future. International Journal of Advanced Computing Science and Engineering, 3(2), 65-72. ISSN 2714-7533

Kineber, A.F., Oke, A.E., Qaralleh, T.J.O., Alaboud, N.S., Alshahrani, A., Alaboud, M. and Daoud, A.O., 2023. Cyber technology implementation barriers for sustainable buildings: A novel mathematical partial least square structural equation modelling. Buildings, 13(4), p.1052.

Kumar, S., Tiwari, P. and Zymbler, M., 2019. Internet of Things is a revolutionary approach for future technology enhancement: a review. Journal of Big Data, 6(1), pp.1-21.

Mahmud, S.H., Assan, L. & Islam, R. (2018). Potentials of Internet of Things (IoT) in Malaysian construction industry. Annals of Emerging Technologies in Computing, 2(4), pp. 44-52.

Mantha, B.R.K. and García de Soto, B. (2019) 'Cyber security challenges and vulnerability assessment in the construction industry', in Proceedings of the Creative Construction Conference 2019, Budapest, Hungary, pp. 29–37. doi:10.3311/ccc2019-005.

Maqbool, R., Saiba, M.R., and Ashfaq, S., 2022. Emerging industry 4.0 and Internet of Things (IoT) technologies in the Ghanaian construction industry: sustainability, implementation challenges, and benefits. Environmental Science and Pollution Research. https://doi.org/10.1007/s11356-022-24764-1

Onososen, A.O., Musonda, I., Onatayo, D., Tjebane, M.M., Saka, A.B. and Fagbenro, R.K., 2023. Impediments to Construction Site Digitalisation Using Unmanned Aerial Vehicles (UAVs). Drones, 7(1), p.45.

Osunsanmi, T.O., Aigbavboa, C. & Oke, A. (2018). Construction 4.0: The future of the construction industry in South Africa. International Journal of Civil and Environmental Engineering, 12(3), 206-212.

Parn, E.A. and Edwards, D. (2019) 'Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence', Engineering, Construction and Architectural Management, 26(2), pp. 245–266. doi:10.1108/ECAM-03-2018-0101.

Rao, A.S. and Lepech, M.D., 2021. Securing the Internet of Things (IoT) in construction: Current status and future directions. Automation in Construction, 128, p.103766.

Rekeraho, A., Cotfas, D.T., Cotfas, P.A., Bălan, T.C., Tuyishime, E. and Acheampong, R. (2023) 'Cybersecurity challenges in IoT-based smart renewable energy', pp. 1–25. Preprint.

Sawyer, T. and Rubenstone, J. (2019) Construction cybercrime is on the rise, ENR. Available at: https://www.enr.com/articles/46832-construction-cybercrime-is-on-the-rise (Accessed: 25 April 2023).

Silva dos Santos, R., and Assayag, E. S., 2022. Internet of Things (IOT) Applied in Construction Industry: A Systematic Review. International Journal of Engineering Technologies and Management Research, 9(12), 23–29. doi: 10.29121/ijetmr.v9.i12.2022.1272

Tang, S., Shelden, D.R., Eastman, C.M., Pishdad-Bozorgi, P. and Gao, X., 2019. A review of building information modeling (BIM) and the internet of things (IoT) devices integration: Present status and future trends. Automation in Construction, 101, pp.127-139. https://doi.org/10.1016/j.autcon.2019.01.020

Tanga, O., Akinradewo, O., Aigbavboa, C. and Thwala, D. (2022) 'Cyber attack risks to construction data management in the fourth industrial revolution era: a case of Gauteng province, South Africa', Journal of Information Technology in Construction (ITcon), 27(41), pp. 845–863. doi:10.36680/j.itcon.2022.041.

Trotter, L., Harding, M., Mikusz, M. and Davies, N., 2018. IoT-Enabled Highway Maintenance: Understanding Emerging Cybersecurity Threats. IEEE Pervasive Computing, 17(3), pp.23-34.

Turk, Ž., Sonkor, M.S. and Klinc, R. (2022) 'Cybersecurity Assessment of BIM/CDE Design Environment Using Cyber Assessment Framework', Journal of Civil Engineering and Management, 28(5), pp. 349–364. doi:10.3846/jcem.2022.16682.

Watson, S. (2018) Cyber-security: What will it take for construction to act?, Construction News. Available at: https://www.constructionnews.co.uk/tech/cyber-security-what-will-it-take-for-construction-to-act-22-01-2018/ (Accessed: 25 April 2023).

Woodhead, R., Stephenson, P. and Morrey, D., 2018. Digital construction: From point solutions to IoT ecosystem. Automation in Construction, 93, pp.35-46. https://doi.org/10.1016/j.autcon.2018.05.004