The Use of Zero Trust Architecture in Construction Data Management: Future Trends and Future Directions

Ornella Tambwe[1], and Clinton Aigbavboa[2]

[1,2] University of Johannesburg, South Africa
tambweorny@gmail.com

Abstract
The construction industry has embraced digitalisation to manage project data and monitor project execution and worker performance daily. However, this digitalisation also creates opportunities for hackers to breach networks and conduct malicious activities. Today, data must be protected not only from external threats, believed to be hackers, but also from trusted stakeholders and internal devices to maintain full control. Therefore, this study aims to highlight the use of zero-trust architecture in enhancing construction data management and to identify the latest trends and key themes to increase awareness within the construction sector. The objective was achieved through a bibliometric review using the Scopus database over a four-year period (2021-2025). A bibliometric analysis was conducted to identify emerging trends and themes. This research was limited to Scopus-indexed peer-reviewed literature in the fields of computer science and engineering. The findings indicate a lack of domain-specific literature, suggesting that while ZTA attracts significant attention in computer cybersecurity, science, and engineering, its application in construction remains largely unexplored. The study underscores the need for ZTA in construction data management and security. It is recommended that construction stakeholders adopt ZTA for secure data management throughout the project lifecycle, as this approach remains new to the industry. Additionally, further training and education are necessary to grasp the ZTA's purpose and its implementation. The value of this research lies in mapping the evolution of this research area for researchers and all construction stakeholders. It also provides a foundation for informed ZTA adoption and future investigations within the construction sector.

Keywords
Construction Industry, Zero Trust, Zero trust architecture, Data management, Data Security.

1. Introduction

The construction industry, like any other sector, is not immune to the shift from traditional data management (paper-based) to new digital data management (Adekunle et al., 2021). This shift was also motivated by the fact that the construction sector is complex and requires a huge amount of data from various sources and locations to prevent work stoppages. Tools such as BIM, drones, and sensors enable the tracking of construction progress, the receipt of real-time data, and the collection of management data (Adwan and Al-Soufi, 2018). Also, the outbreak of COVID-19 forced workers worldwide to switch from on-site or office work to remote work, and this is an exception for the construction sector (Tsai et al., 2024). This further increased the amount of data collected daily, emphasising the importance of data management. Data management is a critical aspect of every project as it ensures a large amount of data availability, accuracy, and consistency to enable better decision-making and ensure project delivery success (Tambwe et al., 2025). Data management is a broad field which also includes data security, in which various techniques and methods are applied to protect data from unauthorised use and manipulation. This field of data management is relevant as companies that have adopted digitalisation are facing security challenges such as hacking, viruses, malware, man-in-the-middle attacks, password cracking, and distributed denial of service (Tanga et al., 2022; Rahman, 2025). To address the various data security measures used, including antivirus software, regular password changing, intrusion prevention systems, and inline DDoS mitigation.

Nevertheless, most data security research focuses on external attackers and neglects insider attackers, as the project stakeholders' relationship is built upon trust, which further gives an avenue to more data insecurities. In this case, a zero-trust architecture is essential for all critical infrastructure and enterprise assets (Syed et al., 2022; Adapa, 2024). The construction sector can be excluded because it enables most critical sectors by maintaining critical infrastructure and involves many assets from start to finish. Therefore, secured construction data management is essential, as compromised construction data can threaten national security. According to Ahmadi (2024), a zero-trust architecture refers to a cyber protection system that emphasises not trusting anyone, aiming to significantly reduce and prevent data breaches. Syed et al. (2022) and Edo et al. (2022) further stressed that, unlike traditional perimeter-based security, which assumes all devices and users inside the network are trustworthy, ZTA is based on enforcing dynamic and strict security policies, granular access control, and the principle of least privilege, highlighting that no user or device is automatically trusted. Khan (2023) added that the adoption of ZTA not only minimises data exposure to criminals but also protects data integrity and improves both threat identification and detection. This is made possible through technologies such as behavioural analytics, multi-factor authentication, data incident reporting, as well as data tokenisation.

The ZTA also faces implementation challenges, including low adoption in the domain of data security due to the knowledge gap, difficulty in operationalising the concept, as well as misleading deductions (Edo et al., 2022). Gambo and Almulhem (2025) highlighted that, although this architecture can be applied across various industries, it encounters hurdles related to scale, complexity, and operational demands. This is because fine-grained access control, large-scale networks, and scalability issues impose management burdens, while real-time authentication and the integration of advanced technologies introduce latency and design challenges. Also, Syed et al. (2022) explained that the different sources from which data is received, including uncertain and numerical information, further complicate the establishment of a trust mechanism capable of efficiently utilising the varying inputs, such as behavioural, device-specific, contextual, and location data. As a result, the adoption of the ZTA remains obscure and requires more research. Gambo and Almulhem (2025) added that organisational barriers, such as cultural resistance, legacy systems, regulatory compliance, and high costs, further complicate deployment. Moreover, resource constraints in IoT devices, policy coordination difficulties, and managing heterogeneous infrastructures make sustaining a robust ZTA framework highly demanding. Federici et al.'s (2023) study addressed the challenges of achieving secure remote access in an Industrial IoT setup by introducing a multi-level authorisation design that enables precise access control and facilitates easier scaling and management of devices. Laghari et al. (2025) explored combining the ZTA and artificial intelligence to combat cyber-attacks, such as intrusions in industrial IoT architecture, while Paul and Rao (2022) discussed the Zero-trust model for smart manufacturing industries. While these research studies address cyber-attacks and their management globally, none of them is directly focused on construction or the built environment. Therefore, the purpose of this study is to emphasise the use of zero-trust architecture in enhancing construction data management, as well as to identify the latest trends and key themes to increase awareness and promote adoption in construction. This allows stakeholders to enforce continuous verification and avoid blind trust when undertaking projects.

2. Methodology

This study utilized a bibliometric review to explore the applications of Zero trust in construction data management. The bibliometric approach was adopted as it facilitates a systematic and quantitative analysis of existing academic literature, thereby identifying research trends, key themes, and significant contributions in this field, as noted by Kumar (2025). The Scopus database was used to gather relevant literature because of its extensive coverage across various academic disciplines and its effectiveness in bibliometric research (Adekunle et al., 2021). Careful consideration was given to the keywords used to gather bibliographic data for the study. This was achieved using two major Boolean operators [“AND” and “OR”], the search protocol for the study was across all fields with a four-year range for initial search [2021-2025]: “Zero Trust Architecture” OR “Zero Trust Security” AND “Data Management” OR “information Management” AND “Construction”. This search produced a total of 100 documents or publications. To refine the selection for relevance, the study was also limited to specific document types, including journal articles, conference papers, and books, ensuring comprehensive representation of the literature on the subject. Furthermore, additional refinement involved filtering by language, specifically focusing on English, and then by publication stage. The publication stage was limited to the final stage; the subject area was restricted to “Computer Science and Engineering”; the language of the document was confined to “English”; and the document type was limited to “Conference paper, Articles, Books”, thereby narrowing the dataset to 57 relevant publications. For the analysis, VOS viewer software was employed to visualise bibliometric networks, including publication per country and keyword co-occurrence. This tool helps identify thematic clusters and map research trends within literature. Furthermore, the software VOSviewer identifies dominant research themes and emerging topics by visualising connections between studies (Hassan and Duarte, 2024). The findings from this bibliometric analysis offer insights into the growing interest in construction data management solutions in construction, emphasising the role of ZTA architecture in enhancing data security.

2.

3. Research Results

3. 1 Annual and Global Distribution of Publications

The Scopus database results reveal the yearly distribution of research papers on the applications of zero-trust architecture in Construction data management across the four-year review period, that is, 2021-2025. A total of 57 documents were retrieved: 18 conference papers, 24 articles and 15 books. Figure 1 shows the annual distribution of publications from 2021 to 2025.

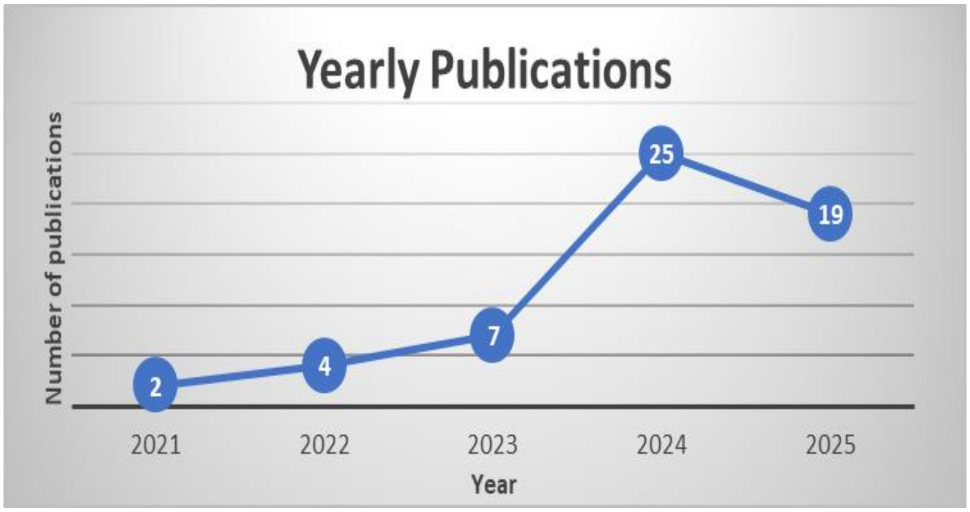

Fig. 1. Annual distribution of Publications

Between 2021 and 2022, a slight increase from 2 to 4 publications indicates a growing interest in this area. Subsequently, a sharp rise from 4 to 25 publications from 2022 to suggests a significant increase in research activity, possibly due to the increased adoption of digital technologies after 2020, which was marked by lockdowns; therefore, people turned to digital means for seeking information, projects, and employee protection. A slight decline to 19 publications from 2024 to 2025 is notable, indicating a drop of 6 documents compared to the previous year. This may be because the year is still ongoing, and more research could still be in progress. This is also supported by Edo et al. (2022), who explained that the ZTA is an emerging security tool requiring more attention and further study in the domain of information and data management.

Only 9 of the 39 countries met the specified criteria of a minimum of two documents and one citation per country. This criterion was set because there is still limited research output on this topic in construction. India had the most significant influence, with 14 documents and 87 citations, followed by China [12 documents, 78 citations] and the UK [7 documents, 53 citations]. Australia, Ireland, and the United States (US) also showed moderate output, each with 3 documents and 48, 47, and 3 citations, respectively. The remaining countries include Bulgaria, Canada, and Saudi Arabia. Although these three countries each had 2 documents, Canada leads in citations with 31, followed by Saudi Arabia with 23, and Bulgaria with 4. Individually, India leads in both documents and citations. Globally, Asia has the most countries publishing on ZTA, followed by Europe and the US, while Africa has no publications meeting the above criterion. Furthermore, Asia also leads in citations, with a total of 188, reflecting significant recognition and impact, likely due to their innovative frameworks and research funding, as noted in Li et al. (2021). Additionally, Africa, with no publication figures, highlights a gap in global collaboration and underscores the insufficient investment and partnerships in developing construction data management and security research in developing countries. Figure 2 illustrates the global distribution of publications discussed.

2.

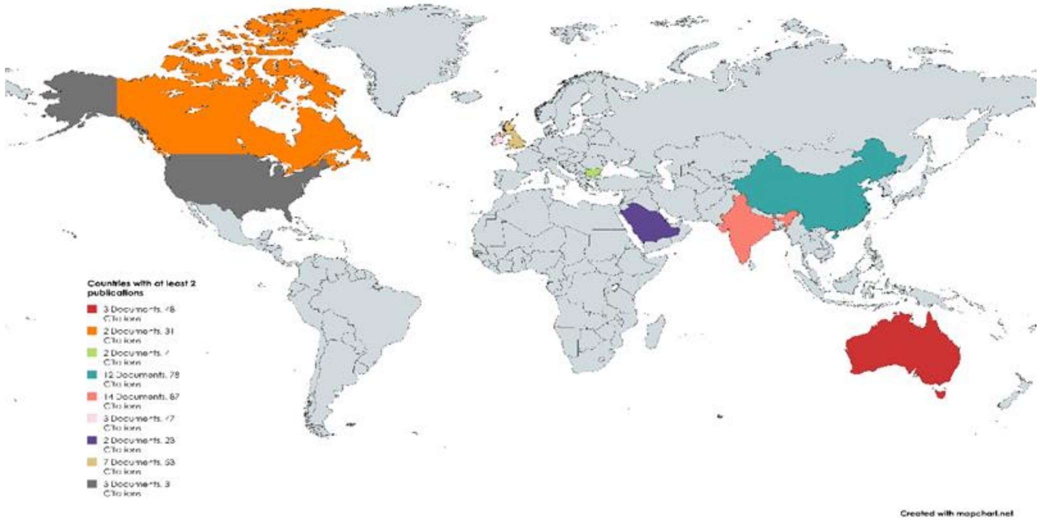

Fig. 2. Global distribution of Publications

4. Research Focus Discussion

A keyword co-occurrence examination was conducted using bibliographic data from the retrieved literature to achieve this. Of the 637 extracted keywords, 28 reached the established threshold of at least three occurrences. However, some terms, such as Blockchain, cybersecurity, case studies, cloud computing, and metaverses, appeared repeatedly with some abbreviations; therefore, some keywords were removed manually, leading to an output of 23 most frequently occurring keywords. As shown in Table 1, the keyword 'Information management' had the highest occurrence, appearing 15 times with a total link strength of 33, establishing it as the central concept around which the other keywords revolve. 'Bloch-chain' and 'Internet of Things' appeared 13 and 10 times with a link strength of 28 and 23, indicating a strong connection between digital tools and data management and security success. 'Network security' had 10 occurrences and a total link strength of 23, underscoring its significance in discussions surrounding Zero trust architecture and construction data protection. 'Cybersecurity,' 'Sensitive data,' and 'Authentication' are less frequent, with 8, 6, and 5 occurrences and total link strengths of 20, 22, and 11, respectively. Nevertheless, they continue to play a significant role in supporting data management functions in the built environment. Table 1. Only display the first five most occurring keywords.

Table1. Research focuses on co-occurring keywords.

Keyword	Occurrences	Total link strength
Information management	15	33
Block-chain	13	28
Internet of things	10	23
Network security	10	25
Cyber security	8	20

These findings demonstrate the increasing use of information management to address data-related issues throughout the construction process, from start to finish. Also, the solid correlation between information management, blockchain, and IoT underscores the value of Information communication tools and technologies, highlighting the various digital tools, skills, and infrastructure needed to achieve data traceability, trust, and security in a data system. Therefore, this implies that there is a need for more tools and technologies education, funding, and policies for the usage of digital security tools to manage and safeguard data against both outsiders and insiders' threats (Jian, 2024). Regarding network security and cybersecurity, there is a growing awareness of digitisation weaknesses in projects involving multiple members, making the zero-trust architecture an ultimate solution.

4.1 Thematic Cluster and Gaps Discussion

2.

A network visualisation map was created with the aid of VosViewer, which indicated that information management is positioned at the centre, while the remaining keywords form interlinked clusters that are the key themes in current construction data management. The network map is displayed below in Figure 2. Emphasises the idea that information management has the ability to transform the overall zero-trust applicability in the construction industry. The map reveals four clusters of keywords. Additionally, the clustered keywords analysis helps to comprehend the correlations between different concepts. The green cluster incorporates keywords such as access control, anonymity, blockchain, metaverse, smart contracts, sustainable development, and trust. The red cluster comprises keywords like big data, cyber-attacks, cybersecurity, deep learning, information management, information security, and threat detection. The yellow cluster includes keywords including artificial intelligence, decision making, and internet of things (IoT). The blue cluster encompasses authentication, cloud computing, network security, privacy, and sensitive data as keywords.

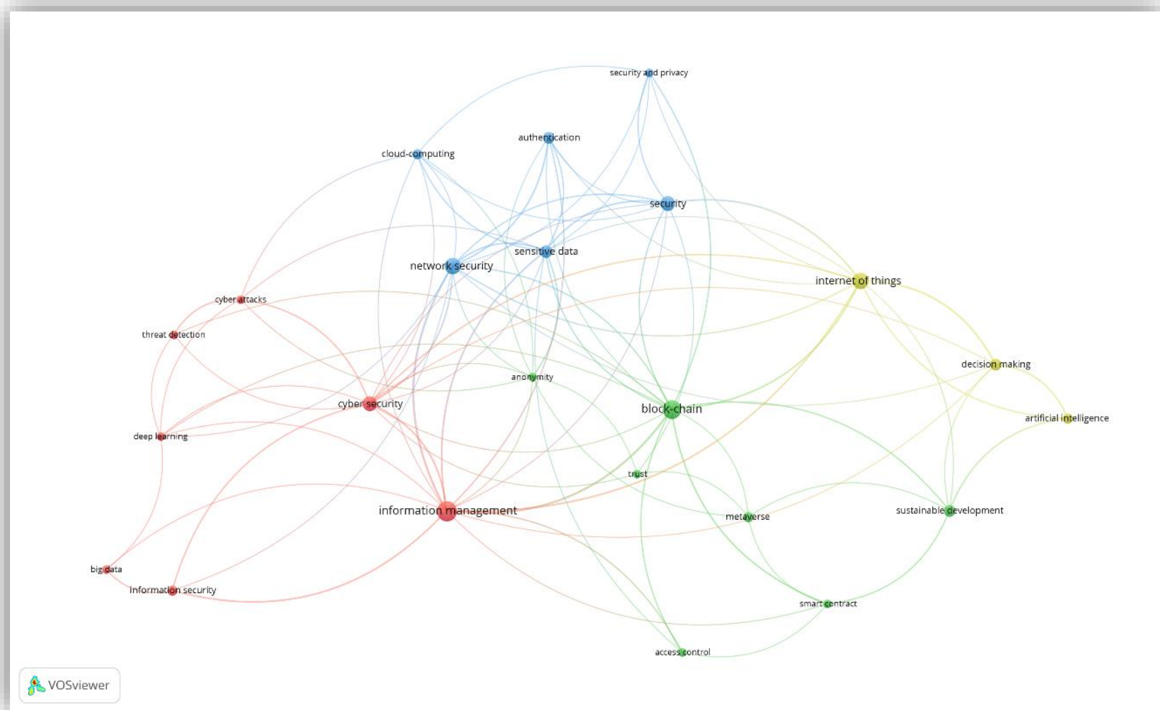

Fig. 2. Network visualisation map

Cybersecurity and Data Intelligence in Construction: Cluster one underlines the role of data-driven intelligence in fighting cyber risks in the construction sector. The integration of big data and deep learning in this cluster emphasises the growing trend of utilising Machine learning and artificial intelligence in various industries to detect and mitigate data threats and manage information, thereby improving behavioural analytics and real-time decision-making capabilities (Gambo and Almulhem, 2025; Laghari et al., 2025). This is an exception for the construction industry, as projects involve continuous management of information and data flow among stakeholders through various ICT tools, including BIM, CAD, IoT sensors, and VR and AR (Adwan and Al-Soufi, 2018). This makes them susceptible to risks, thus requiring principles of zero-trust architecture with data-driven intelligence for real-time validation and constant monitoring of threats. This shows a transition in data security from traditional static security models to a more dynamic approach that evolves as data risks change. Nevertheless, transitioning from concept to practical implementation requires a detailed examination of construction workflows. Successfully adopting ZTA in construction involves a staged approach, beginning with safeguarding the most important assets, including BIM files, project drawings, design revisions, specifications, and financial data, and must be reinforced by worker training to overcome the industry's characteristic cultural resistance to new IT protocols (Lu et al., 2016; Gambo and Almulhem, 2025).

Trust, Access, and Decentralized Technologies: The cluster centres on trust and identity management (access management), which is essential for ZTA. Technologies like smart contracts and Blockchain are vital in both small and large projects, as they ensure efficient workflows, tamper-proof and secure data storage, and foster accountability among project members (Gupta et al., 2023; Gambo and Almulhem, 2025). Edo et al. (2022) emphasised that blockchain-based security frameworks should be integrated with ZTA architectures to enhance security in IoT environments, ensuring high levels of authentication and secure access to both resources and devices. This directly applies to the construction industry. Consider a scenario where a geotechnical subcontractor needs access to foundational BIM data. Under a ZTA framework, their access request initiates a continuous verification process, which authenticates their identity via multi-factor authentication, checks the security status of their device by ensuring that antivirus software is up to date, and permits minimal access only to the exact geotechnical layers of the BIM model for a limited period. The cluster also integrates keywords like sustainable development and anonymity, reflecting the growing interest in establishing robust and sustained data protection within data ecosystems. This aligns with the ZTA guidelines, which focus on identity access controls and decentralised technologies such as blockchain to preserve project data integrity throughout the project execution.

Data Privacy and Cloud Security Management: The inclusion of network security and cybersecurity in this cluster highlights concerns about protecting data from cybercriminals who conduct data breaches and modify data at will. This includes encryption and authentication mechanisms, as well as other security measures such as security automation and segmentation SDN used to help prevent data privacy violations and uncontrolled access (Syed et al., 2022). This work closely aligns with the ZTA, whose aim is to minimise privileged access among stakeholders, emphasising that both systems and users only have access to what is strictly necessary. By doing so, data security through confidentiality and availability is maintained in a distributed cloud environment. Cloud computing is used in the construction environment for stakeholders' collaboration, as it allows access to advanced tools for data management throughout the project execution (Kumar, 2010). Thus, the ZTA is also applicable to construction. Furthermore, Adapa (2024) explained that in a ZTA, factors such as identity management, network segmentation, and monitoring have a significant impact on security; however, data security, which involves protecting information using tools like encryption, digital rights management, and data loss prevention, is also critically important for security. The industry's heavy reliance on cost-sensitive bidding, however, poses considerable financial challenges to implementing such advanced cybersecurity measures in the cloud (Tanga et al, 2022; Tambwe et al., 2025).

AI-driven Decision Making in IoT-enabled Construction: The convergence of AI and IoT is pointed out in this cluster. Due to the hazardous nature of the construction sector, drones, sensors, wearable devices, and robotics are extensively utilised to monitor productivity, worker safety, and weather conditions (Jian, 2024; Khan et al., 2024). However, the difficulty in securing multiple endpoints remains an issue in the build environment, which cybercriminals may exploit if not well protected. This is where the relevance of zero trust lies, as it ensures that all IoT tools are monitored, verified, and limited to explicit tasks, thereby diminishing the occurrence of cyberattacks (Rahman, 2025). However, integrating ZTA with old operational technology and modern IoT sensors on construction sites presents a substantial technical challenge that must be addressed (Aujum and Luz, 2024). Furthermore, the integration of AI in this cluster demonstrates how data collected from IoT can be transformed into actionable insights, which in turn aid in making smarter construction decisions, indicating that security and intelligent systems work closely together (Jian, 2024).

5. Synthesis of the clusters and Gap justification

These clusters suggest that success in modern construction data management depends on integrating technologies like IoT, cybersecurity, network security, and blockchain with zero-trust principles. This shift moves away from security frameworks that viewed anything inside the perimeter as trusted or safe to a resilient, identity-centric model where no one is considered safe, whether inside or outside the network boundary. Consequently, this continuously strengthens the overall project data. However, after a more detailed review, it was observed that there is a lack of domain-specific literature, suggesting that while ZTA is attracting considerable attention in computer cybersecurity, science, and engineering, its application in the construction sector remains underexplored. This is important since the sector is ever more relying on digital platforms, Building Information Modelling (BIM), IoT devices, and cloud-based systems, all of which pose risks to data security. Unlike other industries, such as manufacturing and finance, construction research is significantly behind in adopting ZTA principles for its data management and security practices. This clear disconnect highlights a significant research gap, as ZTA has been acknowledged as a vigorous cybersecurity framework across various fields, but its adaptability, relevance, and ability to reduce insider and outsider threats within construction data ecosystems have not been fully examined. Consequently, this study aims to bridge that gap by evaluating how ZTA can strengthen construction data management practices and exploring trends related to ZTA as well as future research directions for creating resilient, secure, and sustainable digital construction environments.

2.

6. Implications for Construction Data Management

The application of ZTA in data management for construction is a significant development that addresses the environment's unique vulnerabilities and threats in data systems. Although the findings of this research emphasise that ZTA's principles of micro segmentation, continuous verification, and least-privilege access originate from both the engineering and computer science sectors, they are also well-suited to the construction sector. This is because the construction sector includes engineers such as civil, electrical, and geotechnical engineers, among others, and is a sector that involves multi-organisational teams, as well as being faced with extensive cyber-attacks due to Internet of Things tools, and the need to protect BIM data, which is a valuable project asset. Conventional perimeter-based security is no longer effective in this context, as it cannot safeguard data moving across both cloud and organisational boundaries. The ZTA's approach, which promotes the 'never trust, always verify' principle, reduces specific data threats by ensuring every access request, from different engineers or project members to an on-site sensor, is authenticated based on context and identity. This offers the detailed control required to segment sensitive BIM data and secure collaboration channels. The findings of this study significantly influence data risk management, as ZTA can protect against financial loss and operational downtime caused by cyber-hackers while also enhancing physical safety by maintaining the integrity of data that controls automated machinery and on-site systems. Consequently, adopting this adapted framework is essential for a strong and secure future for the construction industry.

7. Conclusion

The study highlights the potential of ZTA to revolutionise construction data management by tackling data protection issues in the digital era. It emphasises that no data risk management method is perfect, so ZTA is also not foolproof; therefore, as risks develop, more security architecture and tools should be designed. However, Construction stakeholders are advised to adopt ZTA for their projects, based on its potential discussed in the study. Additionally, integrating ZTA with IoT and Blockchain can enhance data management and security within the construction industry. The study's limitation stemmed from the scarcity of ZTA publications in the construction sector, necessitating the adaptation of research from other industries. Therefore, researchers in construction should focus on writing about and studying this concept to help the industry fully understand its importance. Another limitation is its reliance on a bibliometric method, which imposes methodological constraints. The findings are based solely on the Scopus database, excluding non-English and non-indexed publications, which may overlook significant ZTA studies and limit the comprehensiveness of the review. Future research should consider using multiple databases to optimise keyword strategies and broaden the scope. Additionally, including bibliometric results validated by construction stakeholders through surveys could strengthen the overall robustness of the findings and the study's applicability. This approach could translate academic insights into practical improvements in data management within the construction industry. Future efforts should focus on developing a construction-specific ZTA framework that combines traditional operational technologies with modern IoT systems, supported by established industry standards and training. The hope of this research is to establish a foundation for more secure, collaborative, and resilient construction projects. If properly implemented, the industry could progress toward a future where sensitive project data is protected by default, trust is consistently verified, and digital innovation is facilitated without compromising security.

References

Adapa, V. R. K. (2024). Zero trust architecture implementation in critical infrastructure: A framework for resilient enterprise security. *International Journal of Advanced Research in Engineering and Technology, 15*(5), 76–89.

Adwan, E., & Al-Soufi, A. (2018). A review of ICT applications in construction. *JOIV: International Journal on Informatics Visualization, 2*(4). https://doi.org/10.30630/joiv.2.4.170

Adekunle, S. A., Aigbavboa, C., Ejohwomu, O., & Thwala, W. D. (2021). Digital transformation in the construction industry: A bibliometric review. *Journal of Engineering, Design and Technology.* https://doi.org/10.1108/JEDT-12-2020-0532

Edo, O. C., Tenebe, T., Etu, E. E., Ayuwu, A., Emakhu, J., & Adebiyi, S. (2022). Zero trust architecture: Trend and impact on information security. *International Journal of Emerging Technology and Advanced Engineering, 12*(7), 140.

2.

Federici, F., Martintoni, D., & Senni, V. (2023). A zero-trust architecture for remote access in industrial IoT infrastructures. *Electronics, 12*(3), 15–20. https://doi.org/10.3390/electronics12030515

Gambo, M. L., & Almulhem, A. (2025). Zero trust architecture: A systematic literature review. *arXiv Preprint.* arXiv:2503.11659. https://doi.org/10.48550/arXiv.2503.11659

Gupta, A., Gupta, R., Jadav, D., Tanwar, S., Kumar, N., & Shabaz, M. (2023). Proxy smart contracts for zero trust architecture implementation in decentralised oracle networks-based applications. *Computer Communications, 206,* 10–21. https://doi.org/10.1016/j.comcom.2023.07.012

Hassan, W., & Duarte, A. E. (2024). Bibliometric analysis: A few suggestions. *Current Problems in Cardiology, 49*(8), 102640. https://doi.org/10.1016/j.cpcardiol.2024.102640

Jain, S. (2024). Bibliometric analysis of Internet of Things (IoT) in the construction industry using Scopus database: Trends, characteristics, and future directions. *Building Engineering, 2*(2), 1503. https://doi.org/10.59400/be.v2i2.1503

Khan, A. M., Alrasheed, K. A., Waqar, A., Almujibah, H., & Benjeddou, O. (2024). Internet of things (IoT) for safety and efficiency in construction building site operations. *Scientific Reports, 14*(1), 28914. https://doi.org/10.1038/s41598-024-28914-y

Kumar, B., Cheng, J. C., & McGibbney, L. (2010, June). Cloud computing and its implications for construction IT. In *Computing in civil and building engineering, Proceedings of the International Conference* (Vol. 30, p. 315). Nottingham University Press.

Kumar, R. (2025). Bibliometric analysis: Comprehensive insights into tools, techniques, applications, and solutions for research excellence. *Spectrum of Engineering and Management Sciences, 3*(1), 45–62.

Laghari, A. A., Khan, A. A., Ksibi, A., Hajjej, F., Kryvinska, N., Almadhor, A., Mohamed, M. A., & Alsubai, S. (2025). A novel and secure artificial intelligence enabled zero trust intrusion detection in industrial internet of things architecture. *Scientific Reports, 15*(1), 26843. https://doi.org/10.1038/s41598-025-26843-3

Li, L., et al. (2021). Mapping the research landscape of nature-based solutions in urbanism. *Sustainability, 13*(7), 3876. https://doi.org/10.3390/su13073876

Paul, B., & Rao, M. (2022). Zero-trust model for smart manufacturing industry. *Applied Sciences, 13*(1), 1–20. https://doi.org/10.3390/app13010001

Rahman, S., & Perumath, N. (2025). Implementing zero trust management in IoT environment—Challenges and solutions: Scoping review. *DiVA Portal.* https://www.diva-portal.org/smash/get/diva2:1955680/FULLTEXT01.pdf

Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (ZTA): A comprehensive survey. *IEEE Access, 10,* 57143–57179. https://doi.org/10.1109/ACCESS.2022.3187426

Tambwe, O. T., Aigbavboa, C. O., Akinradewo, O. I., & Adekunle, P. A. (2025). Measures to address cyber-attacks in construction project data management processes: A cybersecurity perspective. *IET Information Security, 19*(1), 7398742. https://doi.org/10.1049/iet-ifs.2025.7398742

Tanga, O., Akinradewo, O., Aigbavboa, C., & 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, 27,* 281–296. https://doi.org/10.36680/j.itcon.2022.016

Tsai, M., Lee, S., & Shieh, S. W. (2024). Strategy for implementing zero trust architecture. *IEEE Transactions on Reliability, 73*(1), 93–100. https://doi.org/10.1109/TR.2023.3332227

Lu, Q., Won, J. and Cheng, J.C., 2016. A financial decision making framework for construction projects based on 5D Building Information Modeling (BIM). *International Journal of Project Management*, *34*(1), pp.3-21.

Anjum, K.N. and Luz, A., 2024. Investigating the Role of Internet of Things (IoT) Sensors in Enhancing Construction Site Safety and Efficiency. *International Journal of Advances in Engineering and Management*, *6*(463), pp.10-35629.