Sustainable Built Environment, Vol. 225, 2026, 61–70
https://doi.org/10.54941/ahfe1007899

A Data Security Framework: A Step Towards Reducing Data Risks in the Construction Industry

Ornella Tambwe, Clinton Aigbavboa, Toluwanimi Ogunade, Gloria Akanyawie, and Nana Asabea Gyadu-Asiedu

CIDB Centre for Excellence & Sustainable Construction Management and Leadership in the Built Environment, Faculty of Engineering and the Built Environment, University of Johannesburg, South Africa

ABSTRACT

Nowadays, many construction organisations are experiencing data security risks due to the enormous amount of data generated by the adoption of 4IR and the complex nature of the construction sector. These data risks can affect projects to the extent that the company shuts down or abandons the project. The risks include losing important information, extortion, time wastage, cost overruns, and poor project delivery outcomes. For years, construction companies have sought ways to reduce security risks to enable peace of mind throughout the project lifecycle. The adoption of the 4IR (fourth industrial revolution) has raised security risks such as quantum computing threats, viruses, malware, and cyber fraud. Therefore, this study sets out to use the Fourth Industrial Revolution to provide a safe working environment. The study used a literature review methodology to develop knowledge and a framework for how the 4IR can provide security measures in data management. It is evident from the reviewed literature that the 4IR is important for benefits such as fast project delivery and good communication among project members. Moreover, the 4IR is extremely significant for data management during the project lifecycle, promoting better collaboration operations. The various security measures that can be used in the construction sector include using multiple coding methods, digital empowerment of staff, and virus detection software. The study recommended that professionals continue to adopt the 4IR and the data security measures provided in this paper to prevent work delay and stoppage due to risk outbreaks.

Keywords: Construction industry, Data, Data management, Data risks, Data security

INTRODUCTION

Schwab (2017) and Rotatori et al. (2021) explained that the fourth industrial revolution (4IR) began in the twenty-first century, characterised by the prominent presence of technologies such as 3D printing, biotechnology, nanotechnology, energy storage, quantum computing, artificial intelligence, and IoT across various sectors of society. These technologies simplify most of the difficult tasks or jobs that humans used to undertake, including construction projects (Rotatori et al., 2021). Adekunle et al. (2022) emphasised that techniques used in the construction sector include robots, augmented

Received January 8, 2026; Revised February 25, 2026; Accepted March 11, 2026; Available online July 20, 2026

reality, autonomous vehicles, mobile devices, and artificial intelligence. These 4IR tools can aid in managing the vast amounts of information generated, analysed, and stored before, during, and after construction processes. Schwab (2017) and Rotatori et al. (2021) further explained that the 4IR started in the first quarter of the twenty-first century, with technologies like 3D printing, biotechnology, nanotechnology, energy storage, quantum computing, and IoT appearing prominently in society, including in construction. Rotatori et al. (2021) noted that the 4IR not only enables companies to offer services that differentiate them from competitors but also helps restore the natural environment and repair the damage caused by the first three industrial revolutions. Adekunle et al. (2022) stated that 4IR tools enhance service delivery, boost productivity, and support the rapid expansion of construction companies. In the construction sector, the misinterpretation of information, information manipulation, and erasure can impede communication due to the company's size and other issues. Adopting 4IR tools provides many solutions to these challenges (Adekunle et al., 2022). Data and information are vital for the success of every construction company (Tanga et al., 2021a), but managing them presents numerous challenges such as unclear pathways to critical information, data volume, mining and analysis difficulties, unsuitable information systems, unreliable data formats, low data bandwidth, poor data quality, and lack of technological equipment (Adekunle et al., 2022; Tanga et al., 2022a; Tanga et al., 2022b). The use of 4IR tools makes many tasks that humans previously undertook, such as construction projects and data management, more manageable (Rotatori et al., 2021). Unfortunately, many construction organisations are hesitant to adopt these tools due to concerns over data security risks (Van Tam et al., 2024). This research aims to present a 4IR framework for reducing data security risks within the South African construction industry.

FOURTH INDUSTRIAL REVOLUTION IN DATA MANAGEMENT

The 4IR plays a significant role in society because of its benefits for data management, facilitating effective communication and cooperation (Tanga et al., 2021b). The use of large volumes of data (big data) collected from social applications and sensors has proven highly advantageous for many businesses. These benefits are especially evident in data analytics, which helps make informed decisions that enhance competitive advantage over rivals. However, it also raises concerns about data privacy and security, which is a drawback (Nair, 2020). This situation also applies to the construction sector, where vast amounts of data are generated throughout the project lifecycle, and sound decisions are made based on this data. Despite the numerous advantages and roles offered by 4IR tools, their rapid adoption is unlikely because the construction industry tends to resist change and is slow to abandon traditional practices, particularly in underdeveloped and developing countries, as explained by Adekunle et al. (2022). Adoption also faces challenges due to data security risks, since information is managed and shared over the Internet, exposing project and personnel data to hackers (Tanga et al., 2022a). These security risks adversely affect organisations

through time wastage, project delays, financial losses, poor quality of information, and damage to reputation (Tanga et al., 2022b). Data security fundamentally encompasses cybersecurity, which has become crucial in recent years for maintaining public confidence in digital infrastructure whilst safeguarding core principles such as user privacy, freedom, and equality (Faruk et al., 2022). The data security risks identified in this study includes the following.

Staff Illiteracy/Untrained Users

Every individual involved in the construction project is important and should be included in all aspects of the project to ensure better progress (Tanga et al., 2021; Adekunle et al., 2022). This is made possible through the use of information and communication tools, which are also part of the Fourth Industrial Revolution (4IR) tools (Tanga et al., 2022a). However, all staff within a construction organisation need adequate training to handle 4IR tools, address data security threats, avoid sharing passwords, and comply with policies to prevent potential data security risks (Bulgurcu et al., 2010). A lack of education or training can lead employees to compromise computer systems or share security secrets with outsiders, who may easily steal or destroy the company's data (CIOB, 2018). Additionally, they might click on links sent via email. Furthermore, work engagement, which is among the positive emotions people experience at work, is relevant to training and the execution of construction projects. Having a positive attitude towards one's job can significantly enhance internal motivation to share knowledge. Therefore, staff training will depend on employees' ability and motivation to learn (Adekunle et al., 2022).

Viruses and Malware

Tanga et al. (2022b) stressed that in the construction sector, data and information are needed constantly and must be of high quality. This may not always be ensured with the adoption of 4IR tools, as hackers often exploit these systems to install malware on communication tools (such as information systems and computers). Types of malware include viruses, ransomware, worms, bad rabbit, and Trojan horse (Tanga et al., 2022a). These malicious programs are designed to infect project documents stored on systems, duplicate files, steal sensitive information, slow down operations, and even demand extortion by requesting money to keep private information secret (Ilmudeen, 2013; Nyamuchiwa et al., 2022). Beyond malware, other data security risks in the construction industry include extortion, pharming, spamming, phishing, spoofing, spyware, stolen hardware (such as mobile devices or laptops), password sniffing, website defacement, and unauthorised access (Tanga et al., 2022a). Consequently, these security risks can prevent construction organisations from fully utilising many 4IR tools.

Quantum Computing Hacking

The need to maintain and ensure data security has increased significantly with the development of new technologies, given the sensitivity of stored

digital information. Insecure data can lead to data loss through hacking or malware infections, with much more serious consequences (Faruk et al., 2022). Quantum computing is an emerging field that performs calculations based on the principles of quantum mechanics and intersects with disciplines such as mathematics, physics, and computer science (Feynman, 1999; Hassija et al., 2020). This enables faster data processing. Furthermore, Hassija et al. (2020) noted that companies investing in and developing strategies to integrate quantum supremacy into their operations have a significant advantage in capitalising on the future market at this early stage of development. However, the processing speeds of quantum computers are increasing to such an extent that they could theoretically begin to undermine the security measures protecting data. This is due to quantum computing's ability to decode the algorithms that underpin the encryption keys securing important data (Kong et al., 2024). Consequently, this could allow cyber attackers to infiltrate information systems.

Fraud and Unauthorised Access to the Computer System

There are numerous data threats because hackers are developing new methods to gain unauthorised access to data, networks, and programmes to steal sensitive information and carry out fraudulent transactions. This is especially common with phishing through electronic means (Bendovschi, 2015; Vayansky and Kumar, 2018). Phishing is a type of social engineering technique or cybersecurity concern where a hacker tries to fraudulently obtain the sensitive login details of legitimate users by imitating electronic communications from a reputable or public organisation (Tanga et al., 2022a). This issue is particularly pronounced during the COVID-19 period, when remote communication was highly necessary, leveraging 4IR features such as IoT.

Misconfiguration in the Cloud

The primary goal of data or information management in the construction environment is to exchange project data among numerous stakeholders, as well as to secure, store, control, and retrieve it (Tanga et al., 2021a). As a result, construction project participants must pay greater attention to data management because it determines whether a project will succeed or fail and helps avoid unfavourable outcomes. Due to the many benefits outlined in section 2.0, implementing the 4IR (cloud computing) is essential to address the challenges of managing data for building projects (Tanga et al., 2021a). However, Loureiro et al. (2021) noted that organisations today face problems such as cloud misconfigurations, as enterprises rush to switch from centralised to decentralised operations. These misconfigurations stem from human errors and other mistakes, resulting in service disruptions and the leakage of private information, which can expose project details (Coker, 2020). In other words, cloud misconfiguration simply refers to any glitches in the cloud environment that can easily enable hackers to operate and succeed in their malicious missions targeting information systems in the construction industry (Loureiro et al., 2021; Coker, 2020).

Other Security Risks on Construction Projects

The construction industry is a large sector that faces significant data security risks, as it relies heavily on digital applications used daily to support various construction activities. These applications pose security threats, including the potential loss of vital information if hackers manage to infiltrate the computer system, usually through the network. Hackers can seize control of the system and its data, leading to extortion, where ransom is demanded to unlock the system or keep the information secret. The victim faces two risky options: first, using project funds to regain access, risking cost overruns; second, leaving the funds intact and hiring an expert to unlock the system, which could take days, risking project delays beyond deadlines. Additionally, if hackers modify the data within the system, repeated unwanted changes can cause disputes and poor project outcomes, which can harm the company's reputation (Ilmudeen, 2013; Tanga et al., 2021; Tanga et al., 2022; Tepeli, 2021).

RESEARCH METHODOLOGY

This study primarily focuses on data security risks and reviews the fourth industrial revolution, considering the advantages of the 4IR and its implications for security systems in the construction sector. The study employed secondary data to achieve its research aims. Keywords such as data security, data risks, construction industry, and 4IR were used to search for relevant literature in the IEE, ISI Web of Science, Emerald, Taylor and Francis, and SCOPUS databases. These databases were selected because they are among the most well-known and widely used for scientific research. Following the search, over 460 publications were identified and carefully examined for their relevance to this research work. Only 60 articles were deemed suitable for this research, with the search limited to journals and conference publications from 1999 to 2024. Additionally, publications from other data security developers, recognised as authorities in the field, were included. Ultimately, 21 articles were considered significant as they discussed the characteristics of data management, security, and risk management.

EXPLANATION OF THE DATA SECURITY FRAMEWORK

The first raw block of the framework comprises the identified risks related to data, which have been explained on the slides above (staff illiteracy, virus and malware, quantum computing hacking, fraud and unauthorised computer system access, and misconfiguration in the cloud). The middle row shows the critical security programs for the 4IR that can be implemented to address each data risk identified in the first row, as shown in Figure 1. The last row explains the benefits of implementing these security measures.

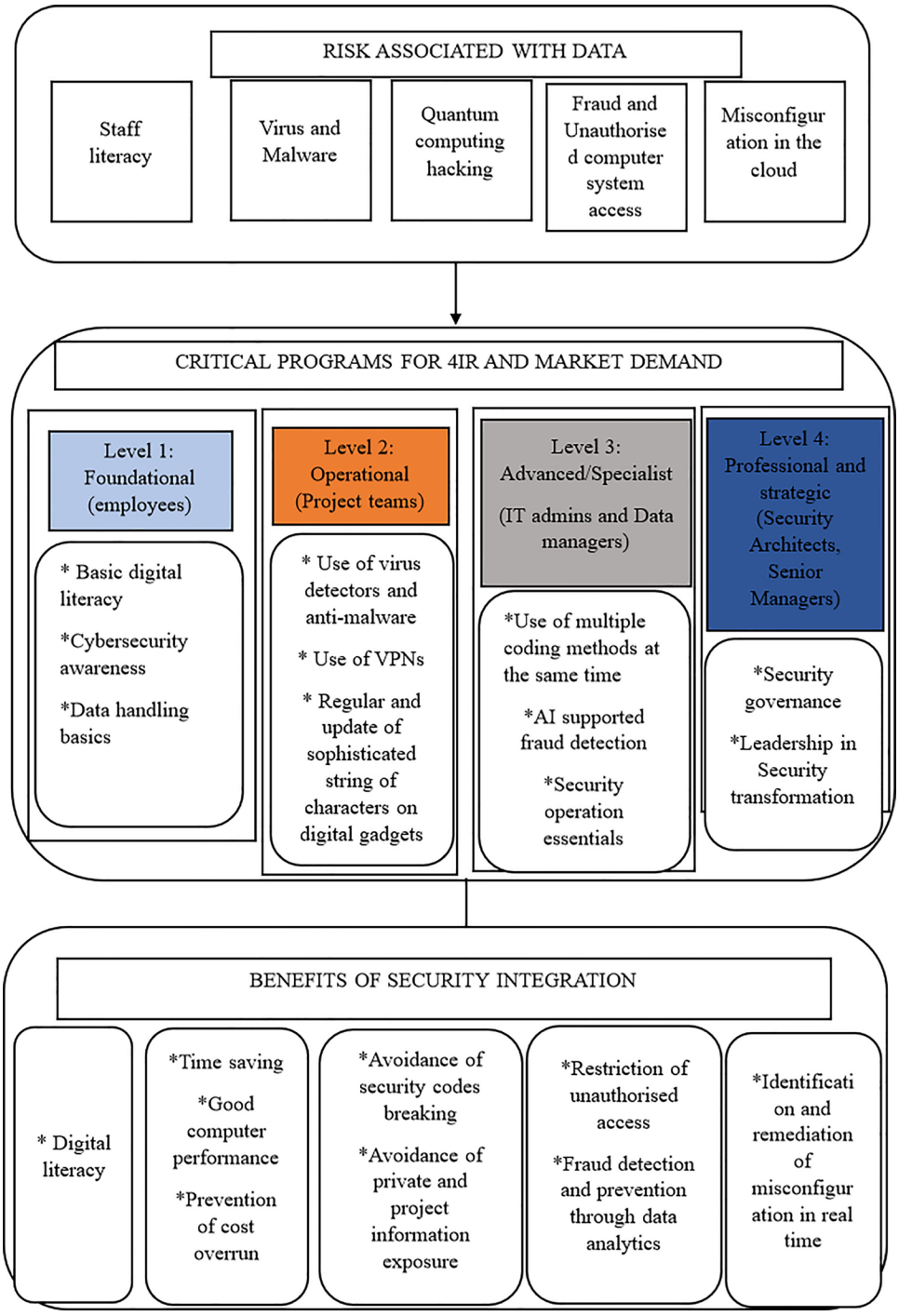

Figure 1: Data risk security using the fourth industrial revolution tools (authors' compilation, 2026).

Based on the developed framework it is shown that staff illiteracy, is mitigated through the implementation of a digital staff empowerment programme that will build capacity tiers. At the foundational level (level 1, named as such), all staff are expected to be literate and possess sufficient knowledge of digital work environments, including email, document control,

and safe device use (CIOB, 2018). The second level, which is the operational level, consists of project members being trained on BIM collaboration practices, mobile field data capture, along with the practical use of virus detection and anti-malware, the use of VPN, and regular updates of sophisticated encryption on digital devices (Konakalla and Veeranki, 2013; Singh and Gupta, 2016; Nyamuchiwa et al., 2022). Furthermore, at the advanced level (level 3), specialist staff, including IT support are expected to have knowledge of the security configuration of platforms, identity and access management, and incident reporting procedures to sustain operational resilience and meet 4IR skill expectations in the market (Tanga et al., 2022a). These methods and software will assist the sector in preventing data loss, saving time, promoting optimal computer performance to meet project delivery timelines, and maintaining effective communication among project members.

For Quantum computing hacking, it can be mitigated by employing multiple coding techniques simultaneously, as well as utilising NIST standards such as Crystals-Kyber, Crystals-Dilithium, Falcon, and Shincs security systems (Rosenquist, 2021; NIST, 2022). These require the capability of levels 3 and 4 for the development of a robust data security architecture. These measures will prevent security code breaches and the exposure of private and project information in the building environment. Additionally, Risks of fraud and unauthorised access to computer systems are being addressed through artificial intelligence, which offers rapid fraud detection and breach prediction, thereby assisting in continuous control over system access (Nyamuchiwa et al., 2022). It is therefore important to emphasise that staff are trained differently at the various levels. For instance, at Level 2, project and finance teams are trained on access request processes and segregation of duties, while at Levels 3 and 4, staff can be trained on security and data analysts receive training on AI-enabled anomaly detection, multi-factor authentication (MFA) policy configuration, and the interpretation of fraud alerts to enable timely response and continuous control over access. Also, to mitigate cloud misconfiguration, erasure coding, access control lists, and secure sockets layer (SSL) are required at the advanced level (Tanga et al., 2021).

The figure thus suggests that adopting this Fourth Industrial Revolution (4IR) tool can restrict unauthorised access, detect and prevent fraud through data analytics. Misconfiguration in the cloud is a problem that can be easily managed through the utilisation of cloud computing (Tanga et al., 2021; Nobles, 2022) through security measures such as erasure coding, access control lists, and secure sockets layer. Moreover, within cloud computing, security measures enable the identification and remediation of misconfigurations in real time.

LESSON LEARNT

Construction project execution has always been a challenging task that requires continuous information management. Managing information now necessitates the use of 4IR tools, as they facilitate all stages of construction

processes. However, the constant use of the internet and Wi-Fi in 4IR adoption puts data at risk, as hackers exploit opportunities to attack construction project information systems, leading to project failures, delays, and other negative consequences. The 4IR is a double-edged sword that offers solutions to improve data communication and project execution,but also heightens data security risks. Conversely, these 4IR technologies address risks that are often overlooked by construction companies. It is recognised that all project members should regard cybersecurity as an essential element of both IT concerns and operational requirements, necessitating a change in mindset and management within the built environment. The study highlights that, to successfully implement the framework, robust training programmes should be offered at various levels of employees. The training includes level 1, mandatory for all stakeholders; level 2 for supervisors and project teams; level 3 for IT specialists; and level 4 for security architects. Additionally, this study provides construction project members with a framework for various risks and strategies to address them, enabling productivity while protecting vital data. This framework was developed and explained to promote and encourage the adoption of 4IR tools across many South African construction organisations. For each risk generated by the 4IR, a countermeasure is presented, along with the benefits that arise from applying these countermeasures. The study emphasises that data risk management should evolve at the same pace as technological advancement, implying that as technology advances, more risk management measures must be implemented to prevent the negative effects of cyberattacks on construction data and projects.

CONCLUSION AND RECOMMENDATION

It is concluded that 4IR tools should be embraced due to their multiple benefits in the construction sector, as they enable better and smoother project execution. Given its importance, the construction sector is encouraged to implement security measures such as digital empowerment, antivirus and malware protection, the use of multiple coding methods, and regular change of password changes. All these security measures should be applied simultaneously to ensure stronger, more effective, and lasting data security. Additionally, adopting data security measures represents a good strategy for ongoing 4IR integration. The study provided four levels of data security training, with level 1 for all stakeholders with access to the project systems, and levels 2 to 4 for higher system permissions and role authorisation. The study also advised that professionals and staff should continue adopting 4IR technologies to prevent delays and unproductivity. Construction parties should be informed about the latest risks and the corresponding data security solutions to ensure success. It is also recommended that top management regularly track training outcomes across all levels, using completion rates and compliance with access reviews. The limitations of this study include its focus on only some data risks; therefore, further research should explore additional data risks. Additionally, the methodology used in this study was a literature review based on secondary data; thus, a quantitative approach should be employed in future research on data security risks to enhance broader applicability.

ACKNOWLEDGMENT

The authors would like to acknowledge the University of Johannesburg, particularly the Department of Construction Management and Quantity Surveying, for its support.

REFERENCES

Adekunle, P., Aigbavboa, C., Akinradewo, O., Oke, A. and Aghimien, D. (2022). Construction information management: Benefits to the construction industry. *Sustainability,* 14(18), pp. 1–17.

Bendovschi, A. (2015). Cyber-attacks: Trends, patterns and security countermeasures. *Procedia Economics and Finance,* 28, pp. 24–31.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly,* 34(3), pp. 523–548.

Coker, J. (2020). Cloud misconfiguration a major compliance risk, say IT decision-makers. *Infosecurity Magazine*. Available at: https://www.infosecurity-magazine.com/news/cloud-misconfigurations-compliance/

Faruk, M.J.H., Tahora, S., Tasnim, M., Shahriar, H. and Sakib, N. (2022). *A Review of Quantum Cybersecurity: Threats, risks and opportunities,* in: Proceedings of the 1st International Conference on AI in Cybersecurity (ICAIC), pp. 1–8. IEEE.

Feynman, R. (1999). Simulating physics with computers (1982), reprinted in: *Feynman and Computation*. Perseus Books.

Hassija, V., Chamola, V., Saxena, V., Chanana, V., Parashari, P., Mumtaz, S. and Guizani, M. (2020). Present landscape of quantum computing. *IET Quantum Communication,* 1(2), pp. 42–48.

Ilmudeen, A. (2013). The impact of computer virus attacks and its preventive mechanisms among personal computer (PC) users, in: *Proceedings of the 3rd International Conference*, 06–07 July 2013, Colombo, Sri Lanka, pp. 97–103. South Eastern University of Sri Lanka.

Kong, I., Janssen, M. and Bharosa, N. (2024). Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions. *Government Information Quarterly,* 41(1), p. 101884.

Loureiro, S. (2021). Security misconfigurations and how to prevent them. *Network Security,* 2021(5), pp. 13–16.

Nair, S.R. (2020). A review on ethical concerns in big data management. *International Journal of Big Data Management,* 1(1), pp. 8–25.

Nobles, C. (2022). Investigating cloud computing misconfiguration errors using human factors analysis and classification system. *Scientific Bulletin,* 27(1), pp. 59–66.

Nyamuchiwa, K., Lei, Z. and Aranas Jr., C. (2022). Cybersecurity vulnerabilities in off-site construction. *Applied Sciences, 12*(10), pp. 1–25.

Rotatori, D., Lee, E.J. and Sleeva, S. (2021). The evolution of the workforce during the fourth industrial revolution. *Human Resource Development International,* 24(1), pp. 92–103.

Schwab, K. (2017). *The fourth industrial revolution*. New York: Crown Publishing Group.

Tanga, O., Akinradewo, O., Aigbavboa, C., Oke, A. and Adekunle, S. (2022b). Data management risks: A bane of construction project performance. *Sustainability,* 14(19), pp. 1–20.

Tanga, O., Akinradewo, O., Aigbavboa, C. and Thwala, D. (2021a). Usage of cloud storage for data management in the built environment, in: *Advances in Artificial Intelligence, Software and Systems Engineering: Proceedings of the AHFE 2021 Virtual Conferences,* July 25–29, 2021, USA, pp. 465–471. Springer International Publishing.

Tanga, O., Akinradewo, O., Aigbavboa, C. and Thwala, D. (2022a). 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, pp. 846–863.

The Chartered Institute of Building (CIOB). (2018). *The role of security in the construction industry.* Available at: https://www.ciob.org/sites/default/files/TheRole of Security in the Construction Industry.pdf.

Vayansky, I. and Kumar, S. (2018). Phishing: challenges and solutions. *Computer Fraud & Security,* 2018(1), pp. 15–20.