Artificial Intelligence, Cyber security and Block chain for Business Intelligence

Micah Oghale Joel [1], Ubamadu Bright Chibunna [2], Andrew Ifesinachi Daraojimba [3*]
[1] Independent Researcher, Ogun State, Nigeria
[2] Signal Alliance Technology Holding, Nigeria
[3] Signal Alliance Technology Holding, Nigeria

* Corresponding Author: **Andrew Ifesinachi Daraojimba**

Article Info

ISSN (online): 2582-7138
Volume: 05
Issue: 01
January-February 2024
Received: 12-12-2023
Accepted: 08-01-2024
Page No: 1383-1387

Abstract
In today's digitally-driven landscape, organizations face increasingly sophisticated cyber threats that demand advanced defensive measures. This review explores the fusion of Artificial Intelligence (AI), Cyber security, Block chain, and Business Intelligence (BI) to fortify organizational security frameworks. Artificial Intelligence has emerged as a pivotal tool in cyber security, empowering systems to detect and respond to threats in real-time. Leveraging AI algorithms, organizations can analyze vast datasets to identify anomalous behavior, predict potential breaches, and automate incident response, thereby bolstering their resilience against evolving cyber threats. The integration of Block chain technology further enhances security by providing a decentralized, immutable ledger that safeguards critical data and transactions. Through Block chain's cryptographic principles, organizations can establish tamper-proof records, ensuring the integrity and authenticity of sensitive information. Business Intelligence complements this synergy by offering valuable insights derived from data analysis, enabling organizations to make informed decisions regarding their security posture. By leveraging BI tools, businesses can identify patterns, trends, and vulnerabilities within their systems, facilitating proactive risk management strategies. This review explores the synergistic potential of integrating AI, Cyber security, Block chain, and BI to create a robust security framework that addresses the multifaceted challenges posed by modern cyber threats. By amalgamating these technologies, organizations can fortify their defenses, mitigate risks, and foster a culture of security-awareness, thereby safeguarding their assets and reputation in an increasingly interconnected digital landscape.

DOI: https://doi.org/10.54660/.IJMRGE.2024.5.1.1383-1387

Keywords: AI; Cyber security; Block chain; Business Intelligence; Review

1. Introduction

In the current cyber security landscape, businesses face increasingly sophisticated threats that target sensitive data, financial assets, and critical infrastructure. The digitization of the economy has led to a surge in cyber-attacks, prompting organizations to adopt advanced technologies to safeguard their operations. Integrating Artificial Intelligence (AI), Cyber security, Block chain, and Business Intelligence (BI) has become imperative to enhance security measures and protect against evolving threats. AI plays a crucial role in cyber security by enabling proactive threat detection and response. AI algorithms can analyze vast amounts of data to identify patterns indicative of cyber threats, enhancing the efficiency and accuracy of cyber security measures (Sharma, 2023). Moreover, AI-based cyber security solutions are essential for detecting and preventing malware, providing a more robust defense mechanism compared to traditional methods (Naeem *et al*., 2022).

Block chain technology offers a decentralized and tamper-resistant platform that enhances cyber security by ensuring data integrity and transparency. Its immutable nature makes it ideal for securing transactions, protecting sensitive information, and preventing unauthorized access (Kshetri, 2017). By leveraging block chain, organizations can establish secure data exchanges,

Enhance identity management, and fortify their cyber security posture (Frederico *et al*., 2021).

Integrating BI into cyber security frameworks enables organizations to make data-driven decisions and gain valuable insights into potential risks and vulnerabilities. BI tools can analyze cyber security data, detect anomalies, and provide actionable intelligence to strengthen security measures (Sarker, 2021). By combining BI with AI and block chain, businesses can create a comprehensive security strategy that leverages data analytics, automation, and secure transactions.

The convergence of AI, Cyber security, Block chain, and BI is essential for addressing the complex challenges posed by cyber threats in the digital age. By harnessing the power of AI for threat detection, block chain for secure transactions, and BI for data-driven insights, organizations can establish a robust cyber security framework that safeguards their assets, data, and operations.

2. Artificial intelligence in cyber security

Artificial Intelligence (AI) significantly enhances cyber security measures through various applications. AI algorithms are utilized in threat detection and response to swiftly identify potential threats and respond proactively (Sadiku *et al*., 2020). These AI-driven systems excel in anomaly detection and predictive analysis, enabling organizations to recognize patterns and behaviors that deviate from the norm (Redino *et al*., 2022). Additionally, the automation of incident response using AI algorithms streamlines the process of handling security incidents, facilitating rapid and efficient mitigation of cyber-attacks (Haider *et al*., 2020).

The integration of AI in cyber security has revolutionized the industry, allowing organizations to modernize security protocols and scale defenses effectively (Jawaid, 2023). By leveraging AI technologies like machine learning and deep learning, cyber security professionals can enhance their capabilities in real-time detection and response to cyber threats (Kaloudi & Li, 2020). While challenges exist, such as concerns regarding bias and trust in AI systems (Parikh *et al*., 2019), efforts are underway to address these issues to ensure the reliability and effectiveness of AI-driven cyber security solutions (Srinivasan & Boer, 2020).

In conclusion, the incorporation of AI in cyber security significantly strengthens organizations' abilities to combat evolving cyber threats. AI algorithms have become indispensable tools in fortifying cyber security defenses, from threat detection and response to anomaly detection and predictive analysis. As AI continues to advance, cyber security professionals must stay updated on the latest developments and best practices to effectively harness the power of AI in safeguarding digital assets.

2.1 Block chain technology in security

Block chain technology is a revolutionary innovation that offers various security features essential for ensuring data integrity and confidentiality. The fundamental principles of block chain, as outlined by (Maldonado-Ruiz *et al*., 2022), include transparency, decentralization, and immutability. These features contribute significantly to the security of the data stored on a block chain network. Decentralization, a core aspect of block chain technology, ensures that there is no single point of failure, as highlighted by (Ahmad *et al*., 2023). This feature enhances security by distributing control across multiple nodes, making it challenging for malicious actors to compromise the system.

Immutability, another critical feature of block chain technology, ensures that once data is recorded on the block chain, it cannot be altered or deleted without broad consensus, as noted by (Fu *et al*., 2018). This immutability feature enhances data integrity and prevents unauthorized modifications, thereby enhancing the security of the information stored on the block chain. Furthermore, the use of consensus mechanisms in block chain networks, ensures that data transactions are validated and added to the block chain in a secure and tamper-proof manner.

In the realm of cyber security, block chain technology finds various applications that leverage its security features. For instance, Alsamhi *et al*. (2021) highlight the use of block chain in combating pandemics by supporting decentralized data, accessibility, and non-repudiation features. Additionally, block chain technology has been applied in healthcare systems to enhance data integrity, transparency, and security, as emphasized by (Elghoul, 2021). The decentralized nature of block chain, coupled with its immutability and auditability, makes it a suitable solution for ensuring trust and security in healthcare data management.

In conclusion, block chain technology's security features, including decentralization, immutability, and transparency, make it a robust solution for enhancing data security and integrity in various domains, including cyber security and healthcare.

2.2 Business intelligence for security enhancement

Business Intelligence (BI) is instrumental in improving security measures within organizations. By utilizing data analysis and visualization techniques, BI facilitates the identification of security trends and patterns, assisting in proactive risk management (Watson, 2009). Decision-makers can effectively access and analyze data through BI tools to make informed decisions that enhance security protocols (Watson, 2009). This strategy aligns with the concept of BI-driven decision-making for proactive risk management, where data-driven insights are employed to fortify security measures (Watson, 2009).

Visualizations are a crucial aspect of BI for enhancing security. Research indicates that effective visualization tools can significantly enhance security analysts' ability to comprehend complex data, leading to improved decision-making processes (Fink *et al*., 2009). Visualization techniques not only help in detecting anomalies in time-series data for root cause analysis but also aid in establishing cyber resilience in embedded systems, which is vital for securing critical infrastructure (Stoffel *et al*., 2013; Siddiqui *et al*., 2019). Additionally, the use of ensemble visualization techniques has been suggested to boost cyber situation awareness in network security data, underscoring the significance of interactive visual representations in understanding security threats (Hao *et al*., 2015).

In the domain of network security, visualizing cyber security data has been a key focus for researchers. Several studies have explored visualizing network anomalies and security logs to equip analysts with effective tools and workspaces to enhance the safety of digital infrastructures (Fink *et al*., 2009; Zhang *et al*., 2017). Moreover, developing visualizations for network attack analysis has been identified as a method to enhance security through efficient data interpretation (Chang & Jeong, 2011).

In summary, integrating BI principles with advanced data analysis and visualization techniques is crucial for organizations seeking to strengthen their security measures. By harnessing BI tools, decision-makers can proactively manage risks, identify security trends, and enhance overall security protocols within their systems.

2.3 Integration of AI, cyber security, block chain, and BI

The integration of Artificial Intelligence (AI), Cyber security, Block chain, and Business Intelligence (BI) presents a synergistic potential that can revolutionize various industries by enhancing security, efficiency, and productivity. By combining AI's predictive capabilities with the secure and transparent nature of block chain technology, organizations can create a comprehensive security framework (Kumar *et al*., 2022). This integration not only addresses multifaceted cyber threats but also offers benefits such as improved performance and security, which traditional systems may lack (Rao & Manvi, 2023).

Researchers have highlighted the transformative impact of integrating block chain and AI in sectors like healthcare, supply chain, and the architecture, engineering, and construction (AEC) industry (Jabarulla & Lee, 2021; Charles *et al*., 2023; Wang *et al*., 2020). For instance, in healthcare, the amalgamation of block chain and AI technologies can democratize and optimize clinical workflows, leading to more efficient and patient-centric healthcare systems (Jabarulla & Lee, 2021). Moreover, the integration of AI and block chain can enhance traceability, security, and efficiency in supply chain operations (Charles *et al*., 2023).

Challenges in integrating AI with block chain, such as security, scalability, and accountability, have been acknowledged (Chithanuru & Ramaiah, 2023; Guergov & Radwan, 2021). However, studies emphasize the importance of overcoming these challenges to leverage the combined potential of these technologies effectively (Salah *et al*., 2019). The fusion of AI and block chain not only enhances data security but also enables explainable and trustworthy AI systems through decentralized and consensus-based decision-making mechanisms (Nassar *et al*., 2019).

Furthermore, the integration of AI, block chain, and IoT has been explored to address security challenges and improve performance in various domains (Koppu *et al*., 2022; Bothra *et al*., 2021). This convergence aims to enhance data security, privacy, and decision-making capabilities in smart environments and IoT devices (Ebrahim *et al*., 2022; Lone *et al*., 2023).

In conclusion, the integration of AI, Cyber security, Block chain, and BI offers a promising avenue for organizations to enhance security, efficiency, and decision-making processes across diverse sectors. By addressing challenges and leveraging the synergistic potential of these technologies, businesses can create robust security frameworks and unlock new opportunities for innovation and growth.

2.4 Challenges and considerations

Artificial Intelligence (AI) cyber security in the context of block chain integration for business intelligence presents several challenges and considerations.

Integrating AI with block chain poses technical challenges such as security, scalability, accountability, and trust in communications (Guergov & Radwan, 2021). The convergence of AI, block chain, and the Internet of Things (IoT) faces challenges related to cyber security, particularly in ensuring data integrity and protection against threats (Mohamed *et al*., 2023). Furthermore, the joint implementation of AI and Block chain Technology (BCT) in supply chains aims to enhance operational performance and sustainability, but it requires overcoming technical hurdles to ensure seamless integration (Tsolakis *et al*., 2022).

Privacy and regulatory considerations are crucial when integrating AI and block chain. Block chain technology can enhance data privacy and security, ensuring overall protection of sensitive information (Alharbi, 2023). However, the integration of AI and block chain in the banking industry raises concerns about privacy breaches and the need for regulatory compliance to safeguard customer data ("The Integration of Artificial Intelligence and Block chain in the Banking Industry: A Critical Practice Based Evaluation of the Present Applications, Adoption, and Future Issues", 2023). Additionally, the ethical implications of AI development, including issues of bias, privacy, accountability, and transparency, must be carefully addressed to ensure responsible AI deployment (Huriye, 2023).

The integration of AI and block chain requires a skilled workforce capable of leveraging these technologies effectively. Training and skill development programs are essential to equip employees with the necessary expertise to work with AI and block chain systems (Kumar *et al*., 2022). Moreover, the adoption of AI in various industries, such as food supply chains, emphasizes the importance of workforce adaptation to leverage AI's capabilities for improving transparency, traceability, and operational efficiency (Dora *et al*., 2021).

In conclusion, the integration of AI cyber security with block chain technology for business intelligence presents technical challenges in terms of security and scalability, privacy concerns that necessitate regulatory compliance, and the need for workforce training and skill development to harness the full potential of these technologies.

2.5 Future trends and outlook

Future trends in Artificial Intelligence (AI), Cyber security, Block chain, and Business Intelligence (BI) are shaping the landscape of technology and organizational practices. The integration of AI, Block chain, and Big Data is revolutionizing various sectors, including smart cities, supply chain management, and the sharing economy (Paiva *et al*., 2021; Su *et al*., 2021; Gurzhiy *et al*., 2022). These technologies are not only enhancing operational efficiency but also enabling new innovative solutions that are changing traditional paradigms (Paiva *et al*., 2021).

Block chain is emerging as a disruptive force in modern businesses, enabling new systems of value and supporting sustainable practices such as supply chain management and digital transformation (Pazaitis *et al*., 2017; Chong *et al*., 2019; Ünalan & Ozcan, 2020). The potential impact of Block chain on organizational security is significant, as it offers secure and transparent transactions, making it a valuable tool for ensuring data integrity and trust in business operations (Chong *et al*., 2019).

Looking ahead, predictions for future developments indicate that Block chain will continue to drive business model innovation, democratize systems of innovation, and impact various industries such as energy, sports, and construction (Lv *et al*., 2022; Papadonikolaki *et al*., 2022). The technology is expected to spread innovation activities across different sectors, making innovation more accessible and efficient (Lv *et al*., 2022). Additionally, the combination of Block chain with other emerging technologies like IoT and AI is set to further transform industries and create new opportunities for growth and development (Gurzhiy *et al*., 2022).

In conclusion, the future outlook for AI, Cyber security, Block chain, and BI is promising, with these technologies expected to drive innovation, enhance security, and revolutionize business practices across diverse sectors. Organizations that embrace these trends and adapt to the changing technological landscape are likely to gain a competitive edge and thrive in the digital era.

3. Recommendation and conclusion

In this discussion, we explored the integration of Artificial Intelligence (AI), Cyber security, Block chain, and Business Intelligence (BI) to create a robust framework for securing digital ecosystems. Key points discussed include the role of AI in enhancing threat detection and response, the security benefits of Block chain technology, and the insights provided by BI for proactive risk management. By combining these technologies, organizations can fortify their defenses, mitigate risks, and foster a culture of security awareness.

Continued innovation and collaboration are essential for staying ahead of evolving cyber threats and ensuring the effectiveness of integrated cyber security frameworks. Organizations must invest in research and development to explore new AI algorithms, Block chain applications, and BI techniques for enhancing security measures. Collaboration among industry stakeholders, academia, and government agencies is crucial for sharing insights, best practices, and threat intelligence to collectively address cyber security challenges. The integrated approach to cyber security, leveraging AI, Cyber security, Block chain, and BI, offers a holistic and proactive strategy for safeguarding digital assets and infrastructure. By harnessing the strengths of each technology, organizations can detect, prevent, and respond to cyber threats more effectively, while promoting transparency, accountability, and inclusivity in security practices. Embracing this integrated approach requires a commitment to ongoing innovation, collaboration, and a culture of security awareness at all levels of the organization.

In conclusion, the integration of AI, Cyber security, Block chain, and BI represents a powerful paradigm shift in cyber security, enabling organizations to adapt to the evolving threat landscape and protect against emerging risks. By leveraging the collective capabilities of these technologies, organizations can build resilient defenses, mitigate risks, and foster trust in the digital ecosystem.

4. References

1. Ahmad R, Salah K, Jayaraman R, Yaqoob I, Ellahham S, Omar M. Block chain and COVID-19 pandemic: applications and challenges. [Preprint]. 2023. Available from: https://doi.org/10.36227/techrxiv.12936572
2. Alharbi A. Applying access control enabled block chain (ACE-BC) framework to manage data security in the CIS system. Sensors. 2023;23(6):3020. https://doi.org/10.3390/s23063020
3. Alsamhi S, Lee B, Guizani M, Kumar N, Qiao Y, Liu X. Block chain for decentralized multi-drone to combat COVID-19 and future pandemics: framework and proposed solutions. Transactions on Emerging Telecommunications Technologies. 2021;32(9). https://doi.org/10.1002/ett.4255
4. Bothra P, Karmakar R, Bhattacharya S, De S. How can applications of block chain and artificial intelligence improve performance of Internet of Things? -- A survey. [Preprint]. 2021. Available from: https://doi.org/10.48550/arxiv.2111.14018
5. Chang B, Jeong C. An efficient network attack visualization using security quad and cube. ETRI Journal. 2011;33(5):770-779. https://doi.org/10.4218/etrij.11.0110.0570
6. Charles V, Emrouznejad A, Gherman T. A critical analysis of the integration of block chain and artificial intelligence for supply chain. Annals of Operations Research. 2023;327(1):7-47. https://doi.org/10.1007/s10479-023-05169-w
7. Chithanuru V, Ramaiah M. An anomaly detection on block chain infrastructure using artificial intelligence techniques: challenges and future directions – A review. Concurrency and Computation: Practice and Experience. 2023;35(22). https://doi.org/10.1002/cpe.7724
8. Chong A, Lim E, Hua X, Zheng S, Tan C. Business on chain: a comparative case study of five block chain-inspired business models. Journal of the Association for Information Systems. 2019:1308-1337. https://doi.org/10.17705/1jais.00568
9. Dora M, Kumar A, Mangla S, Pant A, Kamal M. Critical success factors influencing artificial intelligence adoption in food supply chains. International Journal of Production Research. 2021;60(14):4621-4640. https://doi.org/10.1080/00207543.2021.1959665
10. Ebrahim M, Hafid A, Elie E. Block chain as privacy and security solution for smart environments: a survey. [Preprint]. 2022. Available from: https://doi.org/10.48550/arxiv.2203.08901
11. Elghoul M. A review of leveraging block chain-based framework landscape in healthcare systems. International Journal of Intelligent Computing and Information Sciences. 2021;0(0):1-13. https://doi.org/10.21608/ijicis.2021.75531.1095
12. Fink G, North C, Endert A, Rose S. Visualizing cyber security: usable workspaces. [Preprint]. 2009. Available from: https://doi.org/10.1109/vizsec.2009.5375542
13. Frederico G, Kumar V, Garza-Reyes J, Kumar A, Agrawal R. Impact of I4.0 technologies and their interoperability on performance: future pathways for supply chain resilience post-COVID-19. The International Journal of Logistics Management. 2021;34(4):1020-1049. https://doi.org/10.1108/ijlm-03-2021-0181
14. Fu B, Shu Z, Liu X. Block chain enhanced emission trading framework in fashion apparel manufacturing industry. Sustainability. 2018;10(4):1105. https://doi.org/10.3390/su10041105
15. Guergov S, Radwan N. Block chain convergence: analysis of issues affecting IoT, AI and block chain. International Journal of Computations Information and Manufacturing (IJCIM). 2021;1(1). https://doi.org/10.54489/ijcim.v1i1.48
16. Gurzhiy A, Islam A, Haque A, Marella V. Block chain enabled digital transformation: a systematic literature review. IEEE Access. 2022;10:79584-79605. https://doi.org/10.1109/access.2022.3194004
17. Haider N, Baig M, Imran M. Artificial intelligence and machine learning in 5G network security: opportunities, advantages, and future research trends. [Preprint]. 2020. Available from: https://doi.org/10.48550/arxiv.2007.04490
18. Hao L, Healey C, Hutchinson S. Ensemble visualization for cyber situation awareness of network security data. [Preprint]. 2015. Available from: https://doi.org/10.1109/vizsec.2015.7312766
19. Huriye A. The ethics of artificial intelligence: examining the ethical considerations surrounding the development and use of AI. American Journal of Technology. 2023;2(1):37-45. https://doi.org/10.58425/ajt.v2i1.142
20. Jabarulla M, Lee H. A block chain and artificial intelligence-based, patient-centric healthcare system for combating the COVID-19 pandemic: opportunities and applications. Healthcare. 2021;9(8):1019. https://doi.org/10.3390/healthcare9081019
21. Jawaid S. Artificial intelligence with respect to cyber security. [Preprint]. 2023. Available from: https://doi.org/10.20944/preprints202304.0923.v1
22. Kaloudi N, Li J. The AI-based cyber threat landscape.

ACM Computing Surveys. 2020;53(1):1-34. https://doi.org/10.1145/3372823
23. Koppu S, Kumar K, Somayaji S, Iyapparaja M, Wang W, Su C. Fusion of block chain, IoT and artificial intelligence - a survey. IEICE Transactions on Information and Systems. 2022;E105.D(2):300-308. https://doi.org/10.1587/transinf.2021bcr0001
24. Kshetri N. Block chain's roles in strengthening cyber security and protecting privacy. Telecommunications Policy. 2017;41(10):1027-1038. https://doi.org/10.1016/j.telpol.2017.09.003
25. Kumar S, Lim W, Sivarajah U, Kaur J. Artificial intelligence and block chain integration in business: trends from a bibliometric-content analysis. Information Systems Frontiers. 2022. https://doi.org/10.1007/s10796-022-10279-0
26. Lone A, Mustajab S, Alam M. A comprehensive study on cyber security challenges and opportunities in the IoT world. Security and Privacy. 2023;6(6). https://doi.org/10.1002/spy2.318
27. Lv C, Wang Y, Jaturapitakkul C. The possibility of sports industry business model innovation based on block chain technology: evaluation of the innovation efficiency of listed sports companies. PLOS ONE. 2022;17(1):e0262035. https://doi.org/10.1371/journal.pone.0262035
28. Maldonado-Ruiz D, Torres J, Madhoun N. Fundamentals of block chain technology. Springer Nature Switzerland AG. 2022:3-25. https://doi.org/10.1007/978-3-031-10507-4_1
29. Mohamed N, Oubelaid A, Almazrouei S. Staying ahead of threats: a review of AI and cyber security in power generation and distribution. International Journal of Electrical and Electronics Research. 2023;11(1):143-147. https://doi.org/10.37391/ijeer.110120
30. Naeem M, Khan M, Abdullah A, Noor F, Khan M, Khan M, *et al*. A malware detection scheme via smart memory forensics for Windows devices. Mobile Information Systems. 2022;2022:1-16. https://doi.org/10.1155/2022/9156514
31. Nassar M, Salah K, Rehman M, Svetinovic D. Block chain for explainable and trustworthy artificial intelligence. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. 2019;10(1). https://doi.org/10.1002/widm.1340
32. Paiva S, Ahad M, Tripathi G, Feroz N, Casalino G. Enabling technologies for urban smart mobility: recent trends, opportunities and challenges. Sensors. 2021;21(6):2143. https://doi.org/10.3390/s21062143
33. Papadonikolaki E, Tezel A, Yitmen İ, Hilletofth P. Block chain innovation ecosystems orchestration in construction. Industrial Management & Data Systems. 2022;123(2):672-694. https://doi.org/10.1108/IMDS-03-2022-0134
34. Parikh R, Teeple S, Navathe A. Addressing bias in artificial intelligence in health care. JAMA. 2019;322(24):2377. https://doi.org/10.1001/jama.2019.18058
35. Pazaitis A, Filippi P, Kostakis V. Block chain and value systems in the sharing economy: the illustrative case of Backfeed. Technological Forecasting and Social Change. 2017;125:105-115. https://doi.org/10.1016/j.techfore.2017.05.025
36. Rao K, Manvi S. Survey on electronic health record management using amalgamation of artificial intelligence and block chain technologies. Acta Informatica Pragensia. 2023;12(1):179-199. https://doi.org/10.18267/j.aip.194
37. Redino C, Nandakumar D, Schiller R, Choi K, Rahman A, Bowen E, *et al*. Zero day threat detection using graph and flow-based security telemetry. arXiv. 2022. https://doi.org/10.48550/arxiv.2205.02298
38. Sadiku M, Fagbohungbe O, Musa S. Artificial intelligence in cyber security. International Journal of Engineering Research and Advanced Technology. 2020;6(5):1-7. https://doi.org/10.31695/ijerat.2020.3612
39. Salah K, Rehman M, Nizamuddin N, Al-Fuqaha A. Block chain for AI: review and open research challenges. IEEE Access. 2019;7:10127-10149. https://doi.org/10.1109/ACCESS.2018.2890507
40. Sarker I. Data science and analytics: an overview from data-driven smart computing, decision-making and applications perspective. SN Computer Science. 2021;2(5). https://doi.org/10.1007/s42979-021-00765-8
41. Sharma T. AI-based cyber security threat detection and prevention. IGI Global. 2023:81-98. https://doi.org/10.4018/978-1-6684-9814-9.ch006
42. Siddiqui F, Hagan M, Sezer S. Establishing cyber resilience in embedded systems for securing next-generation critical infrastructure. IEEE SoCC. 2019. https://doi.org/10.1109/SOCC46988.2019.1570548325
43. Srinivasan A, Boer M. Improving trust in data and algorithms in the medium of AI. Maandblad voor Accountancy en Bedrijfseconomie. 2020;94(3/4):147-160. https://doi.org/10.5117/mab.94.49425
44. Stoffel F, Fischer F, Keim D. Finding anomalies in time-series using visual correlation for interactive root cause analysis. SIGMOD Conference. 2013. https://doi.org/10.1145/2517957.2517966
45. Su Z, Zhang M, Wu W. Visualizing sustainable supply chain management: a systematic scientometric review. Sustainability. 2021;13(8):4409. https://doi.org/10.3390/su13084409
46. Tsolakis N, Schumacher R, Dora M, Kumar M. Artificial intelligence and block chain implementation in supply chains: a pathway to sustainability and data monetisation? Annals of Operations Research. 2022;327(1):157-210. https://doi.org/10.1007/s10479-022-04785-2
47. Ünalan S, Ozcan S. Democratising systems of innovations based on block chain platform technologies. Journal of Enterprise Information Management. 2020;33(6):1511-1536. https://doi.org/10.1108/JEIM-07-2018-0147
48. Wang Z, He B, Yu Y, Shen C, Peña-Mora F. Building a next-generation AI platform for AEC: a review and research challenges. arXiv. 2020. https://doi.org/10.46421/2706-6568.37.2020.paper003
49. Watson H. Tutorial: business intelligence – past, present, and future. Communications of the Association for Information Systems. 2009;25. https://doi.org/10.17705/1CAIS.02539
50. Zhang T, Wang X, Li Z, Guo F, Ma Y, Chen W. A survey of network anomaly visualization. Science China Information Sciences. 2017;60(12). https://doi.org/10.1007/s11432-016-0428-2.