Artificial intelligence in cybersecurity: Enhancing threat detection and prevention mechanisms through machine learning and data analytics

[1] Dimple Patil
[1] *Hurix Digital, Andheri, India*

Abstract:

AI in cybersecurity is a disruptive method to addressing the growing sophistication of cyber threats in the digital age. AI-driven technologies like machine learning (ML) and data analytics may improve threat detection and prevention, according to this study. Modern attack vectors including zero-day vulnerabilities, APTs, and ransomware challenge traditional cybersecurity measures. Adaptive learning models and predictive analytics provide proactive threat detection and real-time mitigation with AI. When taught on massive datasets of historical and real-time threat data, machine learning algorithms can find trends and anomalies that rule-based systems miss. IDS and EPP accuracy improves greatly with this feature. AI-powered solutions also automate incident response and dynamic threat hunting, decreasing cyber event detection and containment times. Data analytics aggregates and analyzes logs from multiple sources to provide actionable insights that improve security. Advanced NLP and generative AI have changed threat intelligence by rapidly analyzing cyber threat reports and dark web activities. AI adoption in cybersecurity faces obstacles include algorithmic bias, adversarial attacks on AI models, and hackers misusing AI. Explainable AI (XAI) frameworks are essential for AI-driven cybersecurity transparency and trust. This article brings together AI and cybersecurity trends, tools, and methodologies to discuss predictive threat modeling and proactive protection measures. Industry leaders' case studies show how AI-based solutions can detect and prevent complex assaults. This study emphasizes the necessity for interdisciplinary collaboration to maximize AI's impact on digital ecosystems while resolving ethical and legal issues. The findings support AI-driven cybersecurity to protect vital infrastructure, corporate networks, and personal data in an increasingly linked world.

Keywords: Artificial intelligence, Cybersecurity, Threat detection, Machine learning, Data analytics, Internet of things, Blockchain.

Introduction

The digital age's exponential technology expansion has created unparalleled opportunities and challenging challenges [1-2]. Cybersecurity is one of the biggest issues, especially as cyberattacks become more sophisticated and widespread [1,4-6]. The use of digital systems in finance, healthcare, energy, and national security has increased the demand for threat detection and prevention [7-10]. Traditional cybersecurity methods, while necessary, are failing to address emerging threats. Artificial intelligence (AI) uses machine learning (ML) and data analytics to improve how firms detect, mitigate, and avoid cyber risks [6-7,11-14]. AI in cybersecurity requires a paradigm shift, not just a tool upgrade [15-19]. AI-driven systems learn from data patterns and can detect abnormalities and dangers in real time, unlike predetermined rules and signature-based detection. Machine learning algorithms can find hidden links, zero-day vulnerabilities, and breach-related actions by processing massive amounts of data. This skill is crucial in an era when attackers use ransomware, phishing, and AI to compromise systems.

Machine learning goes beyond detection in cybersecurity [6,20-23]. It helps firms predict hazards via predictive analytics [9,24-28]. Machine learning algorithms can forecast specific breaches and offer countermeasures by studying prior attack data. This predictive capability saves response times and improves resource allocation, reducing operational disruptions and financial losses [29-33]. A subset of AI, natural language processing (NLP), is widely utilized to evaluate textual data from phishing emails and social engineering attempts, adding another layer of defense. Data analytics complements cybersecurity [8,34-38]. The volume and velocity of data generated by modern networks might overwhelm traditional monitoring methods [12,39-43]. Cybersecurity teams can use

AI-powered data analytics to find patterns and connections that might otherwise go undetected. AI-powered systems can detect coordinated attacks across vectors by aggregating and analyzing log data from many sources. This holistic cybersecurity approach increases threat detection, incident response, and forensic investigations.

AI cybersecurity applications are diversifying and growing more complex as it matures [4,44-48]. AI models analyze user and entity behavior to build a baseline of normal activity in behavioral analytics. Any change from this baseline alerts security teams to potential risks. This strategy works well against insider attacks, as bad actors use their legitimate access to compromise systems [18,49-53]. AI-driven systems also improve endpoint security by finding vulnerabilities in linked devices and lowering IoT hazards, an increasing problem. AI cybersecurity adoption is difficult. Data privacy and security are considerations when training machine learning models with large datasets. Adversarial AI, where attackers modify AI models to avoid detection or generate false positives, is as dangerous. Technical advances, strong legal frameworks, and ethical considerations are needed to solve these problems. Industry stakeholders, governments, and academia must work together to responsibly use AI in cybersecurity.

Rapid industry usage of AI in cybersecurity highlights its importance [54-59]. AI-driven cybersecurity solutions increase detection rates, reaction times, and operational costs, according to recent findings. AI-driven security operations centers and automated threat intelligence tools are also being offered by major technology businesses in cybersecurity. Global events and trends influence cybersecurity AI demand [60-64]. Following the COVID-19 outbreak, hybrid work arrangements have increased the attack surface as employees access critical data remotely. AI-powered security technologies are essential for monitoring and safeguarding distributed networks. State-sponsored cyberattacks have increased due to geopolitical tensions, underlining the need for sophisticated threat detection and prevention. AI cannot solve all cybersecurity issues, despite its transformative potential. It must be integrated into a multi-layered security approach that involves human skills, strong policies, and continual monitoring. Interpreting AI insights, fine-tuning models, and responding to complex dangers require human oversight [3,65-69]. Trust in AI-driven systems demands transparency and explainability to reduce biases and ensure stakeholders understand decision-making.

Artificial intelligence in cybersecurity

Interconnected systems, IoT devices, and cloud computing are driving unprecedented cybersecurity vulnerabilities in the digital age [70-74]. Polymorphic malware, ransomware-as-a-service, and advanced persistent threats are used in more sophisticated cyberattacks. In this setting, rule-based and signature-based security solutions no longer protect companies and individuals against changing cyber threats. AI, fueled by ML and data analytics, is revolutionizing cybersecurity by improving threat detection and prevention [75-79]. AI improves cybersecurity by processing vast amounts of data in real time to identify dangers before they become full-scale attacks. AI-driven systems respond dynamically to new threats, unlike traditional methods that use predefined rules and static patterns. Machine learning algorithms can detect small irregularities in network traffic, user behavior, and system activity that may suggest malice. Over time, these systems learn from historical data and attack patterns, enhancing accuracy and efficacy [7,80-83]. Cyber enemies are becoming more sophisticated, making adaptation crucial.

AI's predictive analytics is a major cybersecurity advancement [84-88]. Machine learning-based predictive models can find patterns in previous attack data and anticipate future attack pathways. These methods let companies proactively fix vulnerabilities and increase defenses. Anomaly detection systems can spot strange login attempts or data transfers, which commonly precede cyberattacks [19-20,89-93]. Real-time anomaly detection allows security teams to quickly contain attacks, minimizing the chance of breaches. Artificial intelligence can automate cybersecurity operations including log monitoring, phishing email filtering, and malware analysis in addition to predictive capabilities [94-99]. AI-powered technologies can process massive amounts of data in seconds, freeing up analysts to focus on strategic tasks. Natural language processing (NLP) algorithms can find vulnerabilities and exploits in threat intelligence feeds and unstructured data. Automation improves efficiency and reduces human mistake, which fraudsters exploit.

AI-driven cybersecurity relies on data analytics [100-103]. Organizations can assess their security by combining data from endpoint devices, network logs, and threat intelligence services. Advanced data analytics can find hidden hazards by correlating seemingly unconnected occurrences. A rise in login attempts from a certain region and odd file access patterns may suggest a concerted attack. AI systems can analyse and analyze this data in real time, offering decision-making insights [5,104-106]. Ai-powered cybersecurity solutions are also changing incident response. Manual processes used by incident response teams to investigate and mitigate breaches delayed containment and recovery [107-110]. Companies may automate incident response operations using AI for faster, more effective responses. AI can automatically isolate hacked systems, revoke malicious user rights, and patch vulnerable endpoints. This quick response reduces damage, downtime, and expenses. AI improves endpoint security, another cybersecurity application. As remote work and BYOD rules spread, endpoints are great targets for cyberattacks. AI-driven EPPs and EDRs detect and eliminate device-level threats using machine learning. These tools continuously monitor endpoint activity to detect and prevent malicious processes and applications before they infect the system. AI-powered solutions may also adapt to changing surroundings and user habits, providing strong security across devices and platforms.

AI is changing identity and access management (IAM), a cybersecurity staple [111-113]. Passwords and security tokens are increasingly vulnerable to phishing and credential theft. AI-based biometric identification systems use facial recognition, speech analysis, or behavioral biometrics for greater security. These systems authenticate users using unique physiological or behavioral attributes using machine learning algorithms, making it harder for attackers to spoof legitimate users. AI can also detect and stop real-time unwanted access attempts by analyzing user behavior. AI in cybersecurity faces hurdles despite its many benefits. Adversarial attacks, when cybercriminals alter AI models to avoid detection or produce false positives, are a major problem. Attackers can manipulate data inputs to make AI systems mistake malevolent activities for innocuous. Researchers are investigating adversarial machine learning methods to strengthen AI models against such attacks. To build trust and responsibility, enterprises must make AI-driven systems transparent, explainable, and ethical.

Zero-trust architecture (ZTA) adoption boosts AI's cybersecurity role. Zero-trust concepts stress user and device identity verification and rigorous access limits. Real-time monitoring, risk assessment, and adaptive access management are key to ZTA implementation with AI and ML. Users' location, device type, and access history can be used by AI algorithms to dynamically change access permissions. This lowers the attack surface and counters insider threats and network lateral movement. Federated learning, quantum machine learning, and edge AI will transform cybersecurity with AI. Federated learning allows several businesses to collaborate on model training without disclosing sensitive data, improving security and privacy. Quantum machine learning uses quantum computing to address challenging cybersecurity problems like factoring huge integers for cryptography. Edge AI, which processes data locally on devices rather than in data centers, reduces latency and bandwidth and detects threats faster [2,4,8]. The combination of AI and blockchain technology offers novel ways to secure digital transactions and supply networks [23-26]. Blockchain's immutability and decentralisation complement AI's analytics, enabling secure data sharing and fraud detection. AI can detect irregularities and fraudulent activity in blockchain transaction patterns, improving system integrity. Blockchain can also be used to train AI models with reliable and authentic data.

Public-private partnership will be essential to unlocking AI's full potential as cybersecurity threats increase. To standardize standards, share threat intelligence, and promote AI-driven cybersecurity research and innovation, governments, industry stakeholders, and academics must collaborate. The EU's Cybersecurity Act and CISA's AI working groups are good start. These initiatives strive to develop a secure digital ecosystem that uses AI while resolving its drawbacks. Cybersecurity is crucial as technology evolves and digital transformation permeates society. complex cyber threats including ransomware, phishing, APTs, and state-sponsored cyber espionage necessitate complex countermeasures. Cyberattacks are outpacing static rules and manual oversight-based security solutions. AI, ML, and data analytics improve cybersecurity by detecting and preventing threats faster and more accurately.

Contemporary cyber risks are massive, presenting a problem for enterprises. Data volumes grow exponentially with cloud computing, IoT devices, and remote work. Because modern attacks are so complex, manual monitoring and analysis of this data is impossible. Even automated rule-based systems struggle. AI allows automated, real-

time analysis of massive data sets to uncover security breaches and patterns. This functionality speeds up threat detection and decreases false positives, which security teams have previously faced. Learning and adaptability are AI's cybersecurity benefits. AI systems discover data trends and detect criminal activities using machine learning algorithms, unlike traditional systems that use predefined rules. Supervised learning can be trained on labeled datasets of known cyberattacks to identify future risks. Unsupervised learning can discover network traffic or user behavior anomalies to detect unknown or zero-day threats. This adaptability keeps AI systems successful as cyber threats change.

Another key area where AI thrives is behavioral analytics. AI can identify malicious conduct by evaluating user and system behavior and establishing a "normal" baseline. For instance, an employee accessing sensitive information outside of work hours or from an odd location may prompt further investigation. Insider risks are notoriously hard to identify, but behavioral analytics works well. AI can also analyze contextual elements like device kind and location to better assess threats. AI has revolutionized malware detection. Traditional antivirus systems use signature-based detection, which requires malware understanding. This method fails against polymorphic malware, which often modifies its code to avoid detection. AI-powered systems evaluate file behavior and structure to identify infection independent of previous exposure. These systems detect known and new dangers better using deep learning to identify subtle data patterns and linkages. AI is crucial in fighting phishing assaults, one of the most common cyber risks. Phishing emails are used to steal personal information or install malware. Traditional spam filters are sometimes effective, but fraudsters' strategies are always changing. AI analyzes email content, sender activity, and contextual factors to detect phishing. Natural language processing (NLP) systems can accurately detect phishing indications such strange phrasing, mismatched sender domains, and suspicious attachments.

Security using AI goes beyond threat detection to proactive prevention. Machine learning-powered predictive analytics helps firms identify and eliminate vulnerabilities before they are exploited. AI may evaluate previous attack data to discover adversaries' frequent entry sites and strategies, helping organizations build their defenses. Based on current threat intelligence, predictive models can predict future assaults, helping security teams focus their efforts. AI is also improving incident response. To minimize the threat, mitigate damage, and resume operations, cyber incidents must be addressed quickly. Identifying affected systems, isolating hacked devices, and starting recovery methods are automated by AI, speeding up incident response. AI can detect a ransomware assault and disconnect the afflicted system from the network to stop encryption. Automated responses lessen attack impact by reducing detection and mitigation time.

AI-powered cybersecurity systems are also being linked with SIEM and XDR platforms. Integrations provide a centralized view of an organization's security posture by combining data from numerous sources to understand threats. AI can detect complicated attack patterns by combining endpoint activity, network traffic, and user behavior data. Multi-vector attacks, when attackers use many methods to breach defenses, require such skills. AI-driven IAM systems are another cybersecurity milestone. AI helps enforce strict access rules when firms adopt zero-trust concepts, which believe no user or device can be trusted. AI can alter risk-based access rights by studying user behavior in real time. A person accessing sensitive data from an unknown device may need additional authentication. AI's ability to properly identify individuals based on unique attributes makes biometric authentication technologies like facial recognition and speech analysis a secure alternative to passwords.

AI has tremendous promise in cybersecurity, but it faces hurdles. Using AI, attackers are creating more sophisticated attack methods like phishing emails and malware that adapts to avoid detection. This attacker-defender arms race emphasizes the necessity for creativity and awareness. AI systems' efficiency depends on the quality and amount of their training data. Effective data management is crucial because biased or insufficient datasets can cause threat detection errors or blind spots. Explainability in AI-driven cybersecurity is another issue. AI can provide accurate threat assessments, but its decision-making processes are typically opaque, making it hard for human analysts to interpret or validate its results. Lack of transparency can hurt confidence and adoption, especially in regulated businesses where accountability is key. Explainable AI (XAI) approaches are being developed to improve AI model interpretation and output comprehension. Future technologies like federated learning, quantum computing, and edge AI will improve cybersecurity. Federated learning lets firms train AI models without disclosing sensitive data, enhancing model performance. Quantum computing could break

encryption and enable quantum-resistant algorithms, revolutionizing cryptography. Edge AI computes closer to the data source, speeding threat detection and response in resource-constrained situations like IoT devices.

Conclusions

AI in cybersecurity transforms the fight against emerging cyber threats. Traditional security solutions fail to keep up with cyberattacks' sophistication and volume as the digital landscape gets more complicated. AI's capacity to scan massive datasets in real time and adapt to new attack patterns makes it a crucial threat detection and prevention tool. Machine learning (ML) and data analytics, two key components of AI, may discover abnormalities, predict dangers, and respond to incidents better than previous methods. This paradigm shift emphasizes the need to use cutting-edge AI-driven technology to protect key systems and data in a technical and strategic era of cybersecurity. AI's ability to handle and analyze massive volumes of data in real time is a major cybersecurity advantage. Today's organizations generate massive amounts of sensitive, business-critical data. These datasets' scale and complexity overwhelm traditional threat detection approaches that rely on predetermined rules and human interaction. AI systems excel at detecting patterns and abnormalities that may suggest malice. These systems use advanced machine learning algorithms to detect small risks like anomalous login behaviours or data transfers that conventional tools may miss. This feature increases threat detection accuracy and reduces cyber event response time, which minimizes damage.

Another area where AI is essential is predictive analytics. Machine learning models trained on previous cyberattack data can find trends and anticipate future threats. This proactive approach lets firms block attacks before they happen, improving their security. AI-driven techniques can predict software system vulnerabilities or detect at-risk endpoints, allowing enterprises to prevent them. This game-changer from reactive to proactive cybersecurity strategies gives firms an edge against more sophisticated adversaries. AI automates typical incident response duties, freeing security staff to tackle more difficult issues. Automated threat intelligence platforms can create actionable insights from threat feeds, network logs, and user activity reports. These systems speed up decision-making and guarantee reaction tactics are based on current data. AI-powered tools can also simulate attacks to assess security resilience and uncover vulnerabilities. Such skills can improve security measures and prepare enterprises for new threats.

AI in cybersecurity helps design advanced protection mechanisms that can respond to threats' dynamic nature. AI-driven systems learn and adapt to new attack methods, unlike static security solutions. This agility is crucial for fighting zero-day exploits, which target undiscovered vulnerabilities. AI systems can spot unexpected behaviors or trends that may suggest a zero-day assault using machine learning algorithms and data analytics, allowing enterprises to neutralize the issue before it does substantial damage. In a world where threat actors innovate and improve their approaches, cybersecurity must be dynamic. AI in cybersecurity faces hurdles despite its many benefits. To make these technologies successful and reliable, data privacy, algorithmic bias, and adversarial attacks on AI systems must be addressed. Cybercriminals might modify machine learning model outputs to avoid detection or cause false positives. Adversarial training and explainable AI are being investigated to improve AI system resilience and transparency. To combine security needs with privacy rights, AI monitoring and analysis of user behavior must be ethically balanced.

Implementing and administering AI-driven cybersecurity solutions may require skills. As these technologies advance, AI, data analytics, and cybersecurity experts will be in high demand. Educational programs, interdisciplinary collaboration, and worker training must be developed to close this gap. Organizations can appropriately use AI technologies by developing talent. Several themes will shape AI in cybersecurity in the future. AI, blockchain, quantum computing, and the IoT are expected to combine to improve security. AI-powered blockchain analytics can improve transaction transparency and traceability, while quantum-resistant algorithms can protect systems from quantum threats. Federated learning, which lets AI models be trained on decentralized data without compromising privacy, could also help collaborative cybersecurity initiatives handle data security issues.

References

[1] Tan, P., Chen, X., Zhang, H., Wei, Q., & Luo, K. (2023, February). Artificial intelligence aids in development of nanomedicines for cancer management. In Seminars in cancer biology (Vol. 89, pp. 61-75). Academic Press.

[2] Cheng, K., Li, Z., He, Y., Guo, Q., Lu, Y., Gu, S., & Wu, H. (2023). Potential use of artificial intelligence in infectious disease: take ChatGPT as an example. Annals of Biomedical Engineering, 51(6), 1130-1135.

[3] Wong, F., de la Fuente-Nunez, C., & Collins, J. J. (2023). Leveraging artificial intelligence in the fight against infectious diseases. Science, 381(6654), 164-170.

[4] Barsha, S., & Munshi, S. A. (2023). Implementing artificial intelligence in library services: A review of current prospects and challenges of developing countries. Library Hi Tech News, 41(1), 7-10.

[5] Yanamala, A. K. Y. (2023). Data-driven and artificial intelligence (AI) approach for modelling and analyzing healthcare security practice: a systematic review. Revista de Inteligencia Artificial en Medicina, 14(1), 54-83.

[6] Benvenuti, M., Cangelosi, A., Weinberger, A., Mazzoni, E., Benassi, M., Barbaresi, M., & Orsoni, M. (2023). Artificial intelligence and human behavioral development: A perspective on new skills and competences acquisition for the educational context. Computers in Human Behavior, 148, 107903.

[7] Abdulwahid, A. H., Pattnaik, M., Palav, M. R., Babu, S. T., Manoharan, G., & Selvi, G. P. (2023, April). Library Management System Using Artificial Intelligence. In 2023 Eighth International Conference on Science Technology Engineering and Mathematics (ICONSTEM) (pp. 1-7). IEEE.

[8] Rospigliosi, P. A. (2023). Artificial intelligence in teaching and learning: what questions should we ask of ChatGPT?. Interactive Learning Environments, 31(1), 1-3.

[9] Umamaheswari, S., & Valarmathi, A. (2023). Role of artificial intelligence in the banking sector. Journal of Survey in Fisheries Sciences, 10(4S), 2841-2849.

[10] Patil, D., Rane, N. L., Desai, P., & Rane, J. (2024). Machine learning and deep learning: Methods, techniques, applications, challenges, and future research opportunities. In Trustworthy Artificial Intelligence in Industry and Society (pp. 28-81). Deep Science Publishing. https://doi.org/10.70593/978-81-981367-4-9_2

[11] Sheth, A., Roy, K., & Gaur, M. (2023). Neurosymbolic artificial intelligence (why, what, and how). IEEE Intelligent Systems, 38(3), 56-62.

[12] Rane, J., Kaya, O., Mallick, S. K., & Rane, N. L. (2024). Artificial intelligence in education: A SWOT analysis of ChatGPT and its implications for practice and research. In Generative Artificial Intelligence in Agriculture, Education, and Business (pp. 142-161). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-7-4_4

[13] Rane, J., Kaya, O., Mallick, S. K., & Rane, N. L. (2024). Smart farming using artificial intelligence, machine learning, deep learning, and ChatGPT: Applications, opportunities, challenges, and future directions. In Generative Artificial Intelligence in Agriculture, Education, and Business (pp. 218-272). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-7-4_6

[14] Holzinger, A., Keiblinger, K., Holub, P., Zatloukal, K., & Müller, H. (2023). AI for life: Trends in artificial intelligence for biotechnology. New Biotechnology, 74, 16-24.

[15] Zador, A., Escola, S., Richards, B., Ölveczky, B., Bengio, Y., Boahen, K., ... & Tsao, D. (2023). Catalyzing next-generation artificial intelligence through neuroai. Nature communications, 14(1), 1597.

[16] Rane, J., Kaya, O., Mallick, S. K., Rane, N. L. (2024). Artificial intelligence-powered spatial analysis and ChatGPT-driven interpretation of remote sensing and GIS data. In Generative Artificial Intelligence in Agriculture, Education, and Business (pp. 162-217). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-7-4_5

[17] Rane, J., Mallick, S. K., Kaya, O., & Rane, N. L. (2024). Artificial general intelligence in industry 4.0, 5.0, and society 5.0: Applications, opportunities, challenges, and future direction. In Future Research Opportunities for Artificial Intelligence in Industry 4.0 and 5.0 (pp. 207-235). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-0-5_6

[18] Gašević, D., Siemens, G., & Sadiq, S. (2023). Empowering learners for the age of artificial intelligence. Computers and Education: Artificial Intelligence, 4, 100130.

[19] Bharadiya, J. P., Thomas, R. K., & Ahmed, F. (2023). Rise of Artificial Intelligence in Business and Industry. Journal of Engineering Research and Reports, 25(3), 85-103.

[20] Moor, M., Banerjee, O., Abad, Z. S. H., Krumholz, H. M., Leskovec, J., Topol, E. J., & Rajpurkar, P. (2023). Foundation models for generalist medical artificial intelligence. Nature, 616(7956), 259-265.

[21] Patil, D., Rane, N. L., & Rane, J. (2024). Applications of ChatGPT and generative artificial intelligence in transforming the future of various business sectors. In The Future Impact of ChatGPT on Several Business Sectors (pp. 1-47). Deep Science Publishing. https://doi.org/10.70593/978-81-981367-8-7_1Deep Science Publishing https://doi.org/10.70593/978-81-981367-8-7_1

[22] Rane, J., Mallick, S. K., Kaya, O., & Rane, N. L. (2024). Enhancing black-box models: advances in explainable artificial intelligence for ethical decision-making. In Future Research Opportunities for Artificial Intelligence in Industry 4.0 and 5.0 (pp. 136-180). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-0-5_4
[23] Rane, N. L., & Paramesha, M. (2024). Explainable Artificial Intelligence (XAI) as a foundation for trustworthy artificial intelligence. In Trustworthy Artificial Intelligence in Industry and Society (pp. 1-27). Deep Science Publishing. https://doi.org/10.70593/978-81-981367-4-9_1
[24] Fang, B., Yu, J., Chen, Z., Osman, A. I., Farghali, M., Ihara, I., ... & Yap, P. S. (2023). Artificial intelligence for waste management in smart cities: a review. Environmental Chemistry Letters, 21(4), 1959-1989.
[25] Cooper, G. (2023). Examining science education in ChatGPT: An exploratory study of generative artificial intelligence. Journal of Science Education and Technology, 32(3), 444-452.
[26] Rane, N. L., Desai, P., & Choudhary, S. (2024). Challenges of implementing artificial intelligence for smart and sustainable industry: Technological, economic, and regulatory barriers. In Artificial Intelligence and Industry in Society 5.0 (pp. 82-94). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-1-2_5
[27] Rane, N. L., Kaya, O., & Rane, J. (2024). Artificial intelligence, machine learning, and deep learning technologies as catalysts for industry 4.0, 5.0, and society 5.0. In Artificial Intelligence, Machine Learning, and Deep Learning for Sustainable Industry 5.0 (pp. 1-27). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-8-1_1
[28] Adams, C., Pente, P., Lemermeyer, G., & Rockwell, G. (2023). Ethical principles for artificial intelligence in K-12 education. Computers and Education: Artificial Intelligence, 4, 100131.
[29] Akkem, Y., Biswas, S. K., & Varanasi, A. (2023). Smart farming using artificial intelligence: A review. Engineering Applications of Artificial Intelligence, 120, 105899.
[30] Rane, N. L., Kaya, O., & Rane, J. (2024). Artificial intelligence, machine learning, and deep learning applications in smart and sustainable industry transformation. In Artificial Intelligence, Machine Learning, and Deep Learning for Sustainable Industry 5.0 (pp. 28-52). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-8-1_2
[31] Yüksel, N., Börklü, H. R., Sezer, H. K., & Canyurt, O. E. (2023). Review of artificial intelligence applications in engineering design perspective. Engineering Applications of Artificial Intelligence, 118, 105697.
[32] Rane, N. L., Kaya, O., & Rane, J. (2024). Artificial intelligence, machine learning, and deep learning for enhancing resilience in industry 4.0, 5.0, and society 5.0. In Artificial Intelligence, Machine Learning, and Deep Learning for Sustainable Industry 5.0 (pp. 53-72). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-8-1_3
[33] Patil, D., Rane, N. L., & Rane, J. (2024). Enhancing resilience in various business sectors with ChatGPT and generative artificial intelligence. In The Future Impact of ChatGPT on Several Business Sectors (pp. 146-200). Deep Science Publishing. https://doi.org/10.70593/978-81-981367-8-7_4Deep Science Publishing https://doi.org/10.70593/978-81-981367-8-7_4
[34] Maslej, N., Fattorini, L., Brynjolfsson, E., Etchemendy, J., Ligett, K., Lyons, T., ... & Perrault, R. (2023). Artificial intelligence index report 2023. arXiv preprint arXiv:2310.03715.
[35] Bharadiya, J. (2023). Artificial intelligence in transportation systems a critical review. American Journal of Computing and Engineering, 6(1), 34-45.
[36] Patil, D., Rane, N. L., & Rane, J. (2024). Challenges in implementing ChatGPT and generative artificial intelligence in various business sectors. In The Future Impact of ChatGPT on Several Business Sectors (pp. 107-145). Deep Science Publishing. https://doi.org/10.70593/978-81-981367-8-7_3
[37] von Krogh, G., Roberson, Q., & Gruber, M. (2023). Recognizing and utilizing novel research opportunities with artificial intelligence. Academy of Management Journal, 66(2), 367-373.
[38] Patil, D., Rane, N. L., & Rane, J. (2024). The future of customer loyalty: How ChatGPT and generative artificial intelligence are transforming customer engagement, personalization, and satisfaction. In The Future Impact of ChatGPT on Several Business Sectors (pp. 48-106). Deep Science Publishing. https://doi.org/10.70593/978-81-981367-8-7_2
[39] Jungwirth, D., & Haluza, D. (2023). Artificial intelligence and public health: an exploratory study. International Journal of Environmental Research and Public Health, 20(5), 4541.
[40] Rane, N. L., Rane, J., & Paramesha, M. (2024). Artificial Intelligence and business intelligence to enhance Environmental, Social, and Governance (ESG) strategies: Internet of things, machine learning, and big data analytics in financial services and investment sectors. In Trustworthy Artificial Intelligence in Industry and Society (pp. 82-133). Deep Science Publishing. https://doi.org/10.70593/978-81-981367-4-9_3
[41] Rane, N. L., & Shirke S. (2024). Digital twin for healthcare, finance, agriculture, retail, manufacturing, energy, and transportation industry 4.0, 5.0, and society 5.0. In Artificial Intelligence and Industry in Society 5.0 (pp. 50-66). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-1-2_3
[42] Vora, L. K., Gholap, A. D., Jetha, K., Thakur, R. R. S., Solanki, H. K., & Chavda, V. P. (2023). Artificial intelligence in pharmaceutical technology and drug delivery design. Pharmaceutics, 15(7), 1916.

[43] Rane, N. L., Mallick, S. K., Kaya, O., & Rane, J. (2024). Machine learning and deep learning architectures and trends: A review. In Applied Machine Learning and Deep Learning: Architectures and Techniques (pp. 1-38). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-4-3_1
[44] Rane, N. L., Mallick, S. K., Kaya, O., & Rane, J. (2024). Techniques and optimization algorithms in machine learning: A review. In Applied Machine Learning and Deep Learning: Architectures and Techniques (pp. 39-58). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-4-3_2
[45] George, B., & Wooden, O. (2023). Managing the strategic transformation of higher education through artificial intelligence. Administrative Sciences, 13(9), 196.
[46] Rane, N. L., Mallick, S. K., Kaya, O., & Rane, J. (2024). Techniques and optimization algorithms in deep learning: A review. In Applied Machine Learning and Deep Learning: Architectures and Techniques (pp. 59-79). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-4-3_3
[47] Jan, Z., Ahamed, F., Mayer, W., Patel, N., Grossmann, G., Stumptner, M., & Kuusk, A. (2023). Artificial intelligence for industry 4.0: Systematic review of applications, challenges, and opportunities. Expert Systems with Applications, 216, 119456.
[48] Rane, N. L., Paramesha, M., Rane, J., & Kaya, O. (2024). Emerging trends and future research opportunities in artificial intelligence, machine learning, and deep learning. In Artificial Intelligence and Industry in Society 5.0 (pp. 95-118). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-1-2_6
[49] Yanamala, A. K. Y., & Suryadevara, S. (2023). Advances in Data Protection and Artificial Intelligence: Trends and Challenges. International Journal of Advanced Engineering Technologies and Innovations, 1(01), 294-319.
[50] Rane, N. L., Paramesha, M., Rane, J., & Mallick, S. K. (2024). Policies and regulations of artificial intelligence in healthcare, finance, agriculture, manufacturing, retail, energy, and transportation industry. In Artificial Intelligence and Industry in Society 5.0 (pp. 67-81). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-1-2_4
[51] Zulunov, R., & Soliev, B. (2023). Importance of Python language in development of artificial intelligence. Потомки Аль-Фаргани, 1(1), 7-12.
[52] Patil, D., Rane, N. L., Rane, J., & Paramesha, M. (2024). Artificial intelligence and generative AI, such as ChatGPT, in transportation: Applications, technologies, challenges, and ethical considerations. In Trustworthy Artificial Intelligence in Industry and Society (pp. 185-232). Deep Science Publishing. https://doi.org/10.70593/978-81-981367-4-9_6
[53] Kamalov, F., Santandreu Calonge, D., & Gurrib, I. (2023). New era of artificial intelligence in education: Towards a sustainable multifaceted revolution. Sustainability, 15(16), 12451.
[54] Rane, N. L., Mallick, S. K., Kaya, O., & Rane, J. (2024). Tools and frameworks for machine learning and deep learning: A review. In Applied Machine Learning and Deep Learning: Architectures and Techniques (pp. 80-95). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-4-3_4
[55] Najjar, R. (2023). Redefining radiology: a review of artificial intelligence integration in medical imaging. Diagnostics, 13(17), 2760.
[56] Rane, N. L., Mallick, S. K., Kaya, O., Rane, J. (2024). Emerging trends and future directions in machine learning and deep learning architectures. In Applied Machine Learning and Deep Learning: Architectures and Techniques (pp. 192-211). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-4-3_10
[57] Ooi, K. B., Tan, G. W. H., Al-Emran, M., Al-Sharafi, M. A., Capatina, A., Chakraborty, A., ... & Wong, L. W. (2023). The potential of generative artificial intelligence across disciplines: Perspectives and future directions. Journal of Computer Information Systems, 1-32.
[58] Chen, T. J. (2023). ChatGPT and other artificial intelligence applications speed up scientific writing. Journal of the Chinese Medical Association, 86(4), 351-353.
[59] Ghaffar Nia, N., Kaplanoglu, E., & Nasab, A. (2023). Evaluation of artificial intelligence techniques in disease diagnosis and prediction. Discover Artificial Intelligence, 3(1), 5.
[60] Rane, J., Kaya, O., Mallick, S. K., & Rane, N. L. (2024). Enhancing customer satisfaction and loyalty in service quality through artificial intelligence, machine learning, internet of things, blockchain, big data, and ChatGPT. In Generative Artificial Intelligence in Agriculture, Education, and Business (pp. 84-141). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-7-4_3
[61] Fullan, M., Azorín, C., Harris, A., & Jones, M. (2024). Artificial intelligence and school leadership: challenges, opportunities and implications. School Leadership & Management, 44(4), 339-346.
[62] Rane, J., Kaya, O., Mallick, S. K., & Rane, N. L. (2024). Impact of ChatGPT and similar generative artificial intelligence on several business sectors: Applications, opportunities, challenges, and future prospects. In Generative Artificial Intelligence in Agriculture, Education, and Business (pp. 27-83). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-7-4_2
[63] Hockly, N. (2023). Artificial intelligence in English language teaching: The good, the bad and the ugly. Relc Journal, 54(2), 445-451.
[64] Rane, J., Kaya, O., Mallick, S. K., & Rane, N. L. (2024). Influence of digitalization on business and management: A review on artificial intelligence, blockchain, big data analytics, cloud computing, and internet of things. In Generative

Artificial Intelligence in Agriculture, Education, and Business (pp. 1-26). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-7-4_1

[65] Patil, D., Rane, N. L., & Rane, J. (2024). Future directions for ChatGPT and generative artificial intelligence in various business sectors. In The Future Impact of ChatGPT on Several Business Sectors (pp. 294-346). Deep Science Publishing. https://doi.org/10.70593/978-81-981367-8-7_7

[66] Song, A. H., Jaume, G., Williamson, D. F., Lu, M. Y., Vaidya, A., Miller, T. R., & Mahmood, F. (2023). Artificial intelligence for digital and computational pathology. Nature Reviews Bioengineering, 1(12), 930-949.

[67] Rane, J., Mallick, S. K., Kaya, O., & Rane, N. L. (2024). Automated Machine Learning (AutoML) in industry 4.0, 5.0, and society 5.0: Applications, opportunities, challenges, and future directions. In Future Research Opportunities for Artificial Intelligence in Industry 4.0 and 5.0 (pp. 181-206). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-0-5_5

[68] Fitria, T. N. (2023, March). Artificial intelligence (AI) technology in OpenAI ChatGPT application: A review of ChatGPT in writing English essay. In ELT Forum: Journal of English Language Teaching (Vol. 12, No. 1, pp. 44-58).

[69] Yu, H., & Guo, Y. (2023, June). Generative artificial intelligence empowers educational reform: current status, issues, and prospects. In Frontiers in Education (Vol. 8, p. 1183162). Frontiers Media SA.

[70] Al Kuwaiti, A., Nazer, K., Al-Reedy, A., Al-Shehri, S., Al-Muhanna, A., Subbarayalu, A. V., ... & Al-Muhanna, F. A. (2023). A review of the role of artificial intelligence in healthcare. Journal of personalized medicine, 13(6), 951.

[71] Rane, N. L., Paramesha, M., & Desai, P. (2024). Artificial intelligence, ChatGPT, and the new cheating dilemma: Strategies for academic integrity. In Artificial Intelligence and Industry in Society 5.0 (pp. 1-23). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-1-2_1

[72] Aldoseri, A., Al-Khalifa, K. N., & Hamouda, A. M. (2023). Re-thinking data strategy and integration for artificial intelligence: concepts, opportunities, and challenges. Applied Sciences, 13(12), 7082.

[73] Rane, N. L., Paramesha, M., Rane, J., & Kaya, O. (2024). Artificial intelligence, machine learning, and deep learning for enabling smart and sustainable cities and infrastructure. In Artificial Intelligence and Industry in Society 5.0 (pp. 24-49). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-1-2_2

[74] Patil, D., Rane, N. L., & Rane, J. (2024). Emerging and future opportunities with ChatGPT and generative artificial intelligence in various business sectors. In The Future Impact of ChatGPT on Several Business Sectors (pp. 242-293). Deep Science Publishing. https://doi.org/10.70593/978-81-981367-8-7_6

[75] Ali, S., Abuhmed, T., El-Sappagh, S., Muhammad, K., Alonso-Moral, J. M., Confalonieri, R., ... & Herrera, F. (2023). Explainable Artificial Intelligence (XAI): What we know and what is left to attain Trustworthy Artificial Intelligence. Information fusion, 99, 101805.

[76] Patil, D., Rane, N. L., & Rane, J. (2024). Acceptance of ChatGPT and generative artificial intelligence in several business sectors: Key factors, challenges, and implementation strategies. In The Future Impact of ChatGPT on Several Business Sectors (pp.201-241). Deep Science Publishing. https://doi.org/10.70593/978-81-981367-8-7_5Deep Science Publishing https://doi.org/10.70593/978-81-981367-8-7_5

[77] Malinka, K., Peresíni, M., Firc, A., Hujnák, O., & Janus, F. (2023, June). On the educational impact of chatgpt: Is artificial intelligence ready to obtain a university degree?. In Proceedings of the 2023 Conference on Innovation and Technology in Computer Science Education V. 1 (pp. 47-53).

[78] Ratten, V., & Jones, P. (2023). Generative artificial intelligence (ChatGPT): Implications for management educators. The International Journal of Management Education, 21(3), 100857.

[79] Rane, J., Mallick, S. K., Kaya, O., & Rane, N. L. (2024). Artificial intelligence, machine learning, and deep learning in cloud, edge, and quantum computing: A review of trends, challenges, and future directions. In Future Research Opportunities for Artificial Intelligence in Industry 4.0 and 5.0 (pp. 1-38). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-0-5_1

[80] Noy, S., & Zhang, W. (2023). Experimental evidence on the productivity effects of generative artificial intelligence. Science, 381(6654), 187-192.

[81] Malik, A. R., Pratiwi, Y., Andajani, K., Numertayasa, I. W., Suharti, S., & Darwis, A. (2023). Exploring artificial intelligence in academic essay: higher education student's perspective. International Journal of Educational Research Open, 5, 100296.

[82] Peres, R., Schreier, M., Schweidel, D., & Sorescu, A. (2023). On ChatGPT and beyond: How generative artificial intelligence may affect research, teaching, and practice. International Journal of Research in Marketing, 40(2), 269-275.

[83] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804.

[84] Rane, J., Mallick, S. K., Kaya, O., & Rane, N. L. (2024). Federated learning for edge artificial intelligence: Enhancing security, robustness, privacy, personalization, and blockchain integration in IoT. In Future Research Opportunities for Artificial Intelligence in Industry 4.0 and 5.0 (pp. 93-135). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-0-5_3

[85] Rane, J., Mallick, S. K., Kaya, O., & Rane, N. L., (2024). Scalable and adaptive deep learning algorithms for large-scale machine learning systems. In Future Research Opportunities for Artificial Intelligence in Industry 4.0 and 5.0 (pp. 39-92). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-0-5_2
[86] Gligorea, I., Cioca, M., Oancea, R., Gorski, A. T., Gorski, H., & Tudorache, P. (2023). Adaptive learning using artificial intelligence in e-learning: a literature review. Education Sciences, 13(12), 1216.
[87] Askin, S., Burkhalter, D., Calado, G., & El Dakrouni, S. (2023). Artificial intelligence applied to clinical trials: opportunities and challenges. Health and technology, 13(2), 203-213.
[88] Rane, N. L., Desai, P., & Rane, J. (2024). Acceptance and integration of Artificial intelligence and machine learning in the construction industry: Factors, current trends, and challenges. In Trustworthy Artificial Intelligence in Industry and Society (pp. 134-155). Deep Science Publishing. https://doi.org/10.70593/978-81-981367-4-9_4
[89] Kunduru, A. R. (2023). Effective usage of artificial intelligence in enterprise resource planning applications. International Journal of Computer Trends and Technology, 71(4), 73-80.
[90] Rane, N. L., Desai, P., Rane, J., & Paramesha, M. (2024). Artificial intelligence, machine learning, and deep learning for sustainable and resilient supply chain and logistics management. In Trustworthy Artificial Intelligence in Industry and Society (pp. 156-184). Deep Science Publishing. https://doi.org/10.70593/978-81-981367-4-9_5
[91] Rane, N. L., Kaya, O., & Rane, J. (2024). Advancing the Sustainable Development Goals (SDGs) through artificial intelligence, machine learning, and deep learning. In Artificial Intelligence, Machine Learning, and Deep Learning for Sustainable Industry 5.0 (pp. 73-93). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-8-1_4
[92] Kshetri, N., Dwivedi, Y. K., Davenport, T. H., & Panteli, N. (2024). Generative artificial intelligence in marketing: Applications, opportunities, challenges, and research agenda. International Journal of Information Management, 75, 102716.
[93] Stahl, B. C., Antoniou, J., Bhalla, N., Brooks, L., Jansen, P., Lindqvist, B., ... & Wright, D. (2023). A systematic review of artificial intelligence impact assessments. Artificial Intelligence Review, 56(11), 12799-12831.
[94] Rane, N. L., Kaya, O., & Rane, J. (2024). Human-centric artificial intelligence in industry 5.0: Enhancing human interaction and collaborative applications. In Artificial Intelligence, Machine Learning, and Deep Learning for Sustainable Industry 5.0 (pp. 94-114). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-8-1_5
[95] Mai, G., Huang, W., Sun, J., Song, S., Mishra, D., Liu, N., ... & Lao, N. (2023). On the opportunities and challenges of foundation models for geospatial artificial intelligence. arXiv preprint arXiv:2304.06798.
[96] Rane, N. L., Kaya, O., & Rane, J. (2024). Integrating internet of things, blockchain, and artificial intelligence techniques for intelligent industry solutions. In Artificial Intelligence, Machine Learning, and Deep Learning for Sustainable Industry 5.0 (pp. 115-136). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-8-1_6
[97] Dave, M., & Patel, N. (2023). Artificial intelligence in healthcare and education. British dental journal, 234(10), 761-764.
[98] Rane, N. L., Mallick, S. K., Kaya, O., & Rane, J. (2024). Applications of machine learning in healthcare, finance, agriculture, retail, manufacturing, energy, and transportation: A review. In Applied Machine Learning and Deep Learning: Architectures and Techniques (112-131). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-4-3_6
[99] Rane, N. L., Mallick, S. K., Kaya, O., & Rane, J. (2024). Applications of deep learning in healthcare, finance, agriculture, retail, energy, manufacturing, and transportation: A review. In Applied Machine Learning and Deep Learning: Architectures and Techniques (pp. 132-152). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-4-3_7
[100] Entezari, A., Aslani, A., Zahedi, R., & Noorollahi, Y. (2023). Artificial intelligence and machine learning in energy systems: A bibliographic perspective. Energy Strategy Reviews, 45, 101017.
[101] Soori, M., Arezoo, B., & Dastres, R. (2023). Machine learning and artificial intelligence in CNC machine tools, a review. Sustainable Manufacturing and Service Economics, 2, 100009.
[102] Vanitha, S., Radhika, K., & Boopathi, S. (2023). Artificial Intelligence Techniques in Water Purification and Utilization. In Human Agro-Energy Optimization for Business and Industry (pp. 202-218). IGI Global.
[103] Rane, N. L., Mallick, S. K., Kaya, O., & Rane, J. (2024). Explainable and trustworthy artificial intelligence, machine learning, and deep learning. In Applied Machine Learning and Deep Learning: Architectures and Techniques (pp. 167-191). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-4-3_9
[104] Rane, N. L., Mallick, S. K., Kaya, O., & Rane, J. (2024). From challenges to implementation and acceptance: Addressing key barriers in artificial intelligence, machine learning, and deep learning. In Applied Machine Learning and Deep Learning: Architectures and Techniques (pp. 153-166). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-4-3_8
[105] Su, J., Ng, D. T. K., & Chu, S. K. W. (2023). Artificial intelligence (AI) literacy in early childhood education: The challenges and opportunities. Computers and Education: Artificial Intelligence, 4, 100124.
[106] Soori, M., Arezoo, B., & Dastres, R. (2023). Artificial intelligence, machine learning and deep learning in advanced robotics, a review. Cognitive Robotics, 3, 54-70.

[107] Rane, N. L., Mallick, S. K., Kaya, O., & Rane, J. (2024). Role of machine learning and deep learning in advancing generative artificial intelligence such as ChatGPT. In Applied Machine Learning and Deep Learning: Architectures and Techniques (pp. 96-111). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-4-3_5
[108] Owan, V. J., Abang, K. B., Idika, D. O., Etta, E. O., & Bassey, B. A. (2023). Exploring the potential of artificial intelligence tools in educational measurement and assessment. Eurasia Journal of Mathematics, Science and Technology Education, 19(8), em2307.
[109] Kumar, D., Haque, A., Mishra, K., Islam, F., Mishra, B. K., & Ahmad, S. (2023). Exploring the transformative role of artificial intelligence and metaverse in education: A comprehensive review. Metaverse Basic and Applied Research, 2, 55-55.
[110] Nazer, L. H., Zatarah, R., Waldrip, S., Ke, J. X. C., Moukheiber, M., Khanna, A. K., ... & Mathur, P. (2023). Bias in artificial intelligence algorithms and recommendations for mitigation. PLOS Digital Health, 2(6), e0000278.
[111] Rane, N. L., Kaya, O., & Rane, J. (2024). Advancing industry 4.0, 5.0, and society 5.0 through generative artificial intelligence like ChatGPT. In Artificial Intelligence, Machine Learning, and Deep Learning for Sustainable Industry 5.0 (pp. 137-161). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-8-1_7
[112] Keiper, M. C. (2023). ChatGPT in practice: Increasing event planning efficiency through artificial intelligence. Journal of Hospitality, Leisure, Sport & Tourism Education, 33, 100454.
[113] Sheikh, H., Prins, C., & Schrijvers, E. (2023). Artificial intelligence: definition and background. In Mission AI: The new system technology (pp. 15-41). Cham: Springer International Publishing.

Declarations

Funding: No funding was received.

Conflicts of interest/Competing interests: No conflict of interest.