Obstacles and Impacts of Artificial Intelligence in Digital Security

Mayuting Gao[1,a,*]

[1]Department of Pre-U,Jinan Foreign Language School,Jinan,250031,China
a. enhypen1014@163.com
**corresponding author*

Abstract: This study examines the obstacles and consequences of incorporating artificial intelligence (AI) into digital security in the rapidly evolving digital economy. It emphasizes the importance of safeguarding data in today's digital era, particularly when it comes to international data transfers, and stresses the necessity for effective policies that promote secure and organized data exchange. The study gives analysis through several aspects. For example, it gives analysis of the technical assessment of how block chain technology addresses data security challenges, the impacts of AI on data security, and how data protection standards affect the European digital economy. And the study then shows block chain's vital role in decentralized control over data, emphasizing the complexities of regulating data processors within a highly open and decentralized environment. Furthermore, the study analyses international cooperation regarding cross-border data regulation, suggesting that there is a need for globally recognized legal norms. In conclusion, the study is for that block chain technology is as an essential element, ensuring cross-border data security, and offering technological innovation and legal framework. The findings of this study indicate that the emerging digital age has led to a rise in digital security, including the development of moral and legal issues like deep fakes, exposed human reliability on automation, and disruption of security firms like those involved in robotics.

Keywords: Artificial intelligence, digital security, digital economy, data security.

1. Introduction

Machine intelligence, commonly known as artificial intelligence (AI), encompasses the cognitive abilities demonstrated by machines created by humans. The term artificial intelligence is used to describe the technology that enables conventional computer programs to mimic human intellect.

Natural disasters represent manifestations of uncontrollable natural forces; however, early warning systems can effectively reduce unnecessary casualties. With advancements in technology, the application of AI for predicting natural disasters seems to be moving from theory to reality: Silvia Terra, a San Francisco-based company, utilizes artificial intelligence in forest mapping efforts to provide resources for planners and minimize fire risks. Furthermore, a collaborative project between China University and the China Seismic Administration has led to the development of "smart earthquake" monitoring systems [1] - the world's first personal AI seismic monitoring system capable of accurately estimating parameters related to earthquake source mechanisms within one-second while also assisting in predicting potential tsunami occurrences and strong surges. Data collection regarding past disasters and experiential knowledge have significantly contributed to reducing annual fatalities caused by natural disasters.

The term "digital economy" was first introduced by American scholar Tapscott in his 1996 book "Digital Economy Age," which defined the "era" of the digital economy as an economical form for the application of information technology [2]. The earliest explanation of the concept of a digital economy dates back to a government paper issued by the Ministry of Industry of Japan in May 1997, which clearly states that the basis of information technology, electronic means, and an economy without physical mobility are characteristics of digital finance [3]. The U.S. Department of Commerce's Emerging Digital Economy report, published in July 1998, states that e-commerce and the related technology industries that support e-business are an essential component of the digital economy [4]. It can be seen that early descriptions of the digital economy tended to be equated with e-commerce activities, concepts, and definitions that may be limited to the application of Internet technology at the time. New communications technology and the accelerated integration of traditional economies make it even more challenging to define the concepts of the digital economy.

The digital economy has become a strategic choice to seize the opportunity for a new technological revolution and industrial change. In the thirty-fourth collective study of the Political Bureau of the Central Committee of the Communist Party of China, General Secretary Xi Jinping emphasized that the rapid development of the digital economy, the broad range of radiation, and the profoundness of shadow are becoming a key force in the reorganization of global elements resources, re-shaping the global economic structure and changing global competition patterns. Unlike previous waves of economic globalization, China is no longer just a follower in developing the digital economy but plays a leading role in many areas. As a critical productive element of the digital economy, data elements can play a magnifying, overlapping, and multiplying role in socioeconomic development only when they are fully available. Countries worldwide attach great importance to data, a new type of national strategic asset, and the issue of cross-border data flow security has become the focus of the competitive game of the New Order. On a global scale, while cross-border data flows can significantly improve the efficiency of transnational collaboration, they also face difficulties in coordinating conflicts of interest between economies, increased risks of network security and national security, and data sovereignty violations.

Therefore, it is urgent to make some efficient policies and regulation to balance economic development, protect national interests, and guarantee data security. Furthermore, international cooperation is very important to exchange some ideas to promote digital technology development, and strengthen data security, making digital economy develop well, helpful to global competition patterns, and ensuring all countries benefit from economic globalization.

Data security has emerged as a pivotal concern in an era characterized by rapid global transformation. In this context, the safeguarding of data has become essential not only for the protection of human life and assets but also for its role as a critical resource with widespread implications for societal development and progress; however, data security has been one of the essential issues that have been recognized. effectively protected the safety of human life and property and have also become a vital resource. The Global Times reporter was informed on the 14th that a joint investigation team of the National Computer Virus Response Management Centre and 360 companies had made new progress in the network attack against the Wuhan City Emergency Administration's earthquake monitoring center, finding backdoor malware that corresponded to the characteristics of the U.S. intelligence agencies. The next step will be to openly disclose to the outside world a highly classified global intelligence system of the United States Government, which poses a severe security threat to national security and world peace in our country and the world. According to Chinese experts [5], the network attack by US intelligence agencies on the earthquake monitoring center is a planned and deliberate network military reconnaissance operation that seeks to acquire the ability to analyze, investigate, attribute, and position the country' economic and even military operations. It may lead to social panic and chaos of order. Furthermore, it can be judged that network attack intrusion and theft have become the least costly way for the United States to obtain remote sensing data from other countries. Meanwhile, the US side is also "crying for thieves," claiming that "Chinese hackers are prepared to launch a destructive network attack on critical US infrastructure."Experts reminded that in the face of the increasing trend of aggressiveness, initiative, and aggression in the American concept of network space preparedness, the United States will initiate more network security confrontations. Data security is all about people, from significant to small countries to individuals. Therefore, individuals should not prevent data exchanges or transactions; they should ensure they are safe and lawful.

Addressing the challenges and impacts of AI on data security within the digital economy framework, alongside the rational utilization of policies designed to foster a secure and orderly cross-border data flow, is crucial to leading the globalization of the digital economy. This paper meticulously examines the influence of data security challenges on economic globalization, identifies and addresses the constraints limiting the smooth flow of cross-border data, and offers tailored policy recommendations tailored to China's current data security landscape.

2. Result

The block chain's core technology for decentralized data control (processing) offers the benefit of "decentralized" data processing while also bringing decentralization to the data processor itself [6]. This issue is particularly acute in a fully decentralized public chain where any individual or organization can send data, validate data, and take part in consensus. The traditional regulatory model for data processors faces a significant challenge due to the "zero-threshold" openness of data processing, which has produced many processors.

Moreover, this is because cross-border data control (processing) is a phased procedure that requires data entry, intermediate processing, and cross-border data to be completed. In the data intermediary processing link [7], where a significant volume of data information is managed or processed by a non-local intermediate agency, there will inevitably be a lot of data transaction information [8]. As the foundation for its sanctions, the United States undertook data acquisition using SWIFT controls and monitored worldwide data flows based on those data. Cutting off the connection with SWIFT allows sanctioned States to block cross-border payments. If cross-border data processors are not local institutions, the regulatory State's ability to oversee them significantly diminishes.

However, issues of international cooperation in cross-border data regulation based on block chain. The global international rule of cross-border data regulation follows the basic logic of data regulatory jurisdiction for missing data.

The best way to resolve the rule conflict between the parties in traditional cross-border data flows is to create a global international legal norm for data regulation based on harmonized data governance legislation between European countries [9]. This is because cross-jurisdictional data flows, which involve trans-boundary data flow, require numerous reviews and are in compliance with the data supervision rules of each jurisdiction.

Regional international legal standards are still geographically limited in cross-border data transfers, but global international legal standards are broadly applicable. The United States has adopted the "prohibition of data localization" as a general principle [10], advocating that members should not prohibit or restrict the trans-boundary transfer of information (including personal information) by electronic means by businesses or individuals for commercial purposes, that data localization requirements should be prohibited, and that companies and individuals should not be required to use computing facilities in their own country or to have access to specific data to transact business. On the other hand, the EU adopted a more nuanced approach, contending that local data storage should not result in a trade distortion while respecting the security standards of the nations involved in cross-border transmission. Data security is a top priority for data service providers in many developing nations because they lack the technological capacity to prevent and control network attacks and because there will be greater demands for data localization. Countries including India, Indonesia, and South Africa pushed for data localization and opposed cross-border data flows during the 2019 G20 Summit.

Furthermore, AI social applications have benefited and disadvantaged users as some individuals use their capabilities to harm others. For instance, as more people continue to apply AI in their day-to-day lives, different individuals have taken advantage of the situation, leading to the development of moral and legal issues. As such, this has led people to question the ethical and legal legitimacy of publishing open-source dual-purpose machine-learning algorithms [11]. In this case, the increased adoption of AI has facilitated the ease of altering or cloning videos, images, and sound, an approach that scammers exploit by creating deep fakes. Studies indicate that deep fake cases are likely to increase over the years due to inadequate legal frameworks to control it, the advancing capabilities of AI/ML-generated synthetic content, the increased opportunity for using synthetic content to engage in fraudulent activity, the norms and threshold agreed to by governments, and the susceptibility of the public to believing everything that they see [12]. Therefore, deep fake has made it easier for fraudulent activity to be done as individuals with quality knowledge of AI and the internet can take advantage of vulnerable individuals like older people on the internet.

AI usage has also led to the development of ethical and moral issues on how various technologies are applied. This is based on the gender issue of VPAs as female, which highlights the normative assumptions on the role of women being secondary to men [13]. An excellent example is Siri, where Apple has used a woman’s voice to help its users communicate with their devices.

Research has also shown that AI application is advantageous in various situations. In this case, AI applications need to be regulated so that people can benefit significantly from them. For instance, this has been seen in innovative city development, which revolutionizes urban planning by offering new methods and tools for modeling and analyzing complex urban systems [14]. This has led city planners to make informed decisions and create sustainable, livable, and resilient cities. Through AI, smart cities will efficiently manage the growing urbanization, observe sustainable living by maintaining a green environment and energy consumption, and improve the economic well-being of the people. Moreover, the development of network security threats has promoted a revolutionary change in the field of network protection [15]. Corporations and individuals can observe effective measures to protect themselves from network attacks.

3. Discussion and Conclusion

3.1. Discussion

In the context of the digital era, the rapid development of block chain technology has accelerated technological innovation in the area of cross-border data information. At the same time, the global economy needs technical dynamism to integrate the digital economy with the traditional economy, and the rule of law provides assurances. As the system for trans-boundary data flow changes, the country should also actively investigate the use of block chain technology for cross-border data security and establish a technological fortress for the global cross-bonded data security system. At the same time, it should promote and participate in creating global regulations for data supervision of block chain trans-border payments.

Significantly, the emerging digital age has led to a rise in the number and complexity of network threats, making it hard for individuals and corporations to detect and respond to them effectively. As a result, this has forced governments to figure out how AI can cope with different systems security issues across diverse sectors. As previously mentioned, the active use of AI has questioned the need to resolve different ethical and legal problems. According to recent studies, today's ethical framework in data application is highly blurred, posing risks in promoting data confidentiality [16]. For instance, through increased AI applications in day-to-day activities, many people are at risk of deep fakes as criminals using it as a strategy to engage in fraudulent activities. Through this strategy, many people have lost their money and other valuables to scammers online. Similarly, AI applications have promoted other ethical and moral issues in society, like the gender of VPAs, which are made to sound or act like women, such as Siri [13]. VPAs also perpetuates the existing discriminatory stereotypes of women, whereby they are viewed as lacking the expertise to perform better in certain areas. These views on indirect discrimination have long-term effects on society, mainly how certain genders are associated with particular disciplines and the emergence of the ‘science is for men’ stereotype. Significantly, there is a need to protect women from any form of discrimination, which can be achieved under the Convention on the Elimination of All Forms of Discrimination Against Women. This bias is another obstacle AI faces as it tries to promote data security. Significantly, humans are not heavily affected by biases in some situations despite governments and other bodies implementing measures that need to be observed to minimize bias [17]. This problem appears in AI systems as humans develop and train them. For instance, while creating an AI system, an individual might base their data on biased research, which will be reflected in the AI system.

Increased AI usage in present society is likely to promote increased network breach cases. Technological advancement has caused more people to rely on automation, exposing more human error vulnerabilities [18]. Therefore, advanced developments have been made in AI systems where quality threat detection methods like IDS (unsupervised machine learning intrusion detection systems) are used to address this issue. Given that many people still prefer automation as it is easier to use, other advanced measures have been made by AI developers to ensure that automation enables individuals and organizations to adopt proactive approaches that would recognize, anticipate, and address possible threats [18]. Through this strategy, the need for human intervention is reduced, thereby minimizing human error. As a result, this makes AI usage safer and enables individuals to protect themselves more from any known or unknown threats. Furthermore, the increasing rate of network threats poses a considerable challenge to corporations working in robot security. Through network breaches, people can gain crucial information from these robots, allowing them to engage in any activity or gain access to whatever the robots protect. AI is a double-edged sword, which have advantages and disadvantages. As for the advantage, it can promote revolutionary change in the modern society. For example, based on AIs influence, society will become more convenient, network security management will be improved, and some operation process will be easier.

AI development depends on technological development, and its development can result in complex security challenges, as well as many opportunities. As for its challenges, when human beings become more and more relied on AI in daily life, they will meet with challenges and threats caused by it. Based on some findings in the study, the author gets the conclusion that there is a need of making comprehensive security measures, guaranteeing transparency in decision-making, and maintaining monitoring, which are playing an important role in AI security. Besides, it is important to protect AI development from other dangerous environment, and AI developers must follow some strict regulations and take some security measures during the process of AI development, which can be assessed by third-party AI vendors to ensure that all data aligns with security standards.

3.2. Conclusion

In conclusion, the study shows that AI has both advantages and disadvantages. For instance, based on AI applications, criminals have taken advantage of the situation, leading to increased cases of network threats. An excellent example of this is deep fakes, which are often used to commit fraudulent activities, especially against vulnerable individuals like older people. Similarly, AI development has led to the rise of moral and legal issues. As a result, this has led people to question the ethical and legal legitimacy of publishing open-source dual-purpose machine-learning algorithms. For instance, AI use has facilitated the gender issue of VPAs being portrayed as female, highlighting the normative assumptions on the role of women being secondary to men. Another impact of AI on data security is that it promotes increased network breach cases. Technological advancement has caused more people to rely on automation, exposing more human error vulnerabilities. This has led to quality data security measures to be observed as advanced developments have been made in AI systems where threat detection methods like IDS are used to address this issue.

Based on the results mentioned above, future research needs to reinforce the existing theories and develop new ones as they try to understand the impacts of AI on other sectors, including small and medium enterprises (SMEs). This consideration should be made because SMEs are one of the areas that many people can easily relate to as they interact with them regularly. More research should also be done on the impacts of AI on sparse resources and intermediate economies of less developed and peripheral regions.

References

[1] Uncle, V. (2021). The world's first artificial-intelligent earthquake surveillance system, "Smart Earth Movement," arrives, can touch the earthquakes in one second https://baijiahao.baidu.com/s?id=1697357117680275368&wfr=spider&for=pc

[2] Tapscott, T. (1996). The digital economy: Promise and peril in the age of networked intelligence. New York: McGraw-Hill.

[3] Wang, T. (2021). Dialysis Day Electronics Business [EB/OL]. http://www.cnw.com.cn/issues/2000/15/1512.asp.

[4] Li Junjiang, He Xiaoyin. (2005). Economics and Management Studies. American Digital Economy Analysis, (07), 13-18.

[5] Feng, Y., Ding, Y., & Yuan, H. (2023). The Chinese side locked the network into the Wuhan earthquake monitoring center; expert: the attackers have obvious military reconnaissance purposes.

[6] Aguilera, R.V., Desender, K., Bednar, M.K., Lee, J.H. (2015). Connecting the Dots: Bringing External Corporate Governance into the Corporate Governance Puzzle. Academy of Management Annals, 9 (1), 483-573.

[7] Zheng X., Cai Z. (2020). Privacy-preserved data sharing towards multiple parties in industrial IoTsIEEE J. Sel. Areas Commun., 38 (5), 968-979.

[8] Wu, C. (2022). Anti-monopoly regulatory study of data monopoly behavior,https://kns.cnki.net/kcms2/article/abstract?v=3uoqIhG8C475KOm_zrgu4lQARvep2SAkaWjBDt8_rTOnKA7PWSN5MAIp3EKsR0AjParARQratDZaVq78jgbAUumCyEQwzQ-I&uniplatform=NZKPT

[9] Jiao, H. (2023). Study on the Compliance of Transboundary Data Flow Regulations with International Economic and Trade Rules https://kns.cnki.net/kcms2/article/abstract?v=3uoqIhG8C475KOm_zrgu4sq25HxUBNNTmIbFx6y0bOQ0cH_CuEtpsDrUt8FeK2skrtAUYvRZbu1Q0UGt3TAvarzIpHQ7jaJF&uniplatform=NZKPT

[10] Gao, M. (2022). Study on legal regulations relating to the transboundary movement of personal data https://xuewen.cnki.net/CMFD-1022450654.nh.html

[11] Nikolskaia, K., & Naumov, V. (2020). Ethical and legal principles of publishing open source dual-purpose machine learning algorithms. 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). https://doi.org/10.1109/itqmis51053.2020.9322897

[12] Homeland Security. (2023). Increasing threat of Deepfake identities. https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf

[13] Loideain, N. N., & Adams, R. (2020). From Alexa to Siri and the GDPR: The gendering of virtual personal assistants and the role of Data Protection Impact Assessments. Computer Law & Security Review, 36. https://doi.org/10.1016/j.clsr.2019.105366

[14] Ullah, Z., Al-Turjman, F., Mostarda, L., & Gagliardi, R. (2020). Applications of artificial intelligence and machine learning in Smart Cities. Computer Communications, 154, 313–323. https://doi.org/10.1016/j.comcom.2020.02.069

[15] Dawson, M. (2021). networksecurity impacts for artificial intelligence use within industry 4.0. Scientific Bulletin, 26(1), 24–31. https://doi.org/10.2478/bsaft-2021-0003

[16] Khisamova, Z. I., Begishev, I. R., & Sidorenko, E. L. (2019). Artificial Intelligence and Problems of Ensuring network Security. International Journal of network Criminology, 13(2), 564–577. https://www.proquest.com/openview/a0f125d3f2115d338e180961818a409d/1?pq-origsite=gscholar&cbl=55114

[17] Manyika, J., Silberg, J., & Presten, B. (2019). What do we do about the biases in AI? Harvard Business Review. https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai

[18] Alhayani, B., Jasim Mohammed, H., Zeghaiton Chaloob, I., & Saleh Ahmed, J. (2021). The effectiveness of artificial intelligence techniques against network security risks applies to the IT industry. Materials Today: Proceedings. https://doi.org/10.1016/j.matpr.2021.02.531