Ethical Challenges in Applications of Artificial Intelligence (AI) for Information Security

Aseel hamoud Hamza[1], Sabreen ali Hussein[2], Wurood Mahdi sahib[3], Noor Kadhim Khdhairi[4]

1 College of Law /University of Babylon / Babylon, Iraq
2 College of Basic Education /University of Babylon / Babylon, Iraq
3 College of Medicine /University of Babylon / Babylon, Iraq
4 College of Science for Women /University of Babylon / Babylon, Iraq

DOI: https://doi.org/10.56293/IJASR.2024.6124

IJASR 2024
VOLUME 7
ISSUE 5 SEPTEMBER - OCTOBER **ISSN: 2581-7876**

Abstract: The integration of the use information security with artificial intelligence is a positive necessity to enhance security, reduce human dependence and detect threats. However, this is not without negatives, such as its exploitation for electronic attacks and the use of discrimination, which in turn leads to unfair or wrong results and the deprivation of rights. Therefore, it is necessary to provide treatment, transparency and determine the responsibility arising from errors in applications. This requires a legal framework to protect rights and determine responsibilities.

Keywords: Artificial Intelligence, Information Security, Data Protection, Ethical Challenges.

1. Introduction

Artificial intelligence is rapidly growing with huge programs in regions together with health and security. In healthcare, it is utilized to aid choice-making and enhance painting performance, but this comes with sophisticated moral issues. Despite its capability to enhance fitness, an extra cautious technique is wanted to make sure moral layout. There isn't any complete framework for developing AI in healthcare, with issues such as bias and privacy safety are nonetheless unresolved. Algorithm builders need to remember the potential risks and construct systems that can come across and counter fraud [19]. Actual case studies emphasize the ethical issues associated with using AI in applications such as healthcare considering patient privacy and algorithmic bias are extremely important. Regulations and suggestions are important for the moral deployment of AI in safety to address dangers like fraud and discrimination. Proactive measures are vital to deal with moral challenges posed by using AI programs and uphold man or women's rights and privacy inside the evolving landscape of information security [21].

1.1 Related Work

They have a look to explore how artificial intelligence can adopt human biases through the evaluation of natural languages. The research showed that algorithms trained on natural language facts ought to seize and transmit biases related to race and gender, elevating issues approximately using AI in touchy programs. The researchers highlight the importance of developing algorithms that detect and correct those biases to ensure extra honest and equitable structures. [6]. They examine club inference assaults on gadget-mastering models, where attackers can decide whether a particular statistics sample can be used to teach the model. The attack exploits differences inside the version's responses to educated versus new data. The research suggests that even superior device getting-to-know models are liable to these attacks, posing a chance to data privacy and highlighting the want for more potent protection strategies. [8] The look discusses the absence of a right to explanation for automatic selection-making below the General Data Protection Regulation. The authors explain that the regulation does now not explicitly guarantee this right, and the protections it gives are confined to imparting standard records about the good judgment behind computerized selections instead of an entire clarification of personal decisions. They highlighted felony gaps and discussed the want for a clearer legal framework to make certain transparency in choices made using computerized structures. [10]. The take a look at examines the idea of version interpretability in synthetic intelligence and uncovers a few myths surrounding it. The creator argues that version interpretability isn't always a sincere procedure, and a few complex fashions may also stay tough to understand despite interpretive tools. The studies highlight that those who specialize in version interpretability have to know the associated challenges and

boundaries, in preference to counting on simplified principles that may be deceptive. [14]. They explore the capacity of malicious uses of synthetic intelligence and provide forecasts, prevention strategies, and mitigation processes. The authors discuss how AI may be exploited for dangerous purposes, which include cyberattacks or disinformation campaigns. The research emphasizes the want for proactive measures and collaborative efforts to cope with those dangers and ensure the accountable development and use of AI technology. [15].

2. Impact Artificial Intelligence in Information Security

Artificial Intelligence cybersecurity strategies have developed from automating simple obligations to addressing complex threats through gaining knowledge of data and detecting patterns and anomalies. Initially, AI was used to detect simple threats, however as threats have become extra complicated, machine mastering became famous for enhancing the system's overall performance. These algorithms support predictive analytics to predict and prevent security breaches. This evolution has led to increased use of AI in areas such as NLP.[27]

From the positives, Artificial Intelligence has the potential to enhance the effectiveness of organizations' incident response and enhance information security through rapid data processing, threat identification, and automation of security responses. AI is one of the best technologies to improve information security, outperforming traditional systems in confronting threats. It can process and analyze large amounts of data quickly to detect anomalous behaviors that indicate security breaches.[2]

Artificial Intelligence enhances cybersecurity by automating incident response, implementing preventative measures, and analyzing attacks. It also helps with post-incident analysis, such as the COiN program used to detect fraud at JPMorgan Chase, to improve security.[26]

3. Ethical Challenges in Artificial Intelligence

3.1 Privacy Data

It is to preserve the personal data of individuals from being utilized by other people by accessing sensitive data in unauthorized ways. On the other hand, security ensures the particularity of this data and not adjusting it, with the possibility of it being obtainable at all times and places. With developed technology, information is available in huge quantities and demands transmission and storage, so potent security measures ought to be taken to protect it from security breaches.

Attacks on personal information have increased and become a project for agencies across all sectors. In addition, regulatory frameworks like California Consumer Privacy Act and GDPR have accelerated legal obligations to protect data and its privacy. Therefore, there is a need to provide security measures such as encryption and data masking to mitigate or eliminate various threat factors [24]. Safety has become a crucial challenge, especially concerning safeguarding the privacy of data in sensitive environments. Thus, several techniques have been utilized, including encryption and data masking to mitigate or eliminate various threat factors [22]

In the areas of AI and autonomous driving applications, the integration of privacy and transparency is important. Malicious attacks can lead to traffic violations, underscoring the importance of protecting privacy. In the healthcare sector, malicious data can distort AI models and influence treatment recommendations. In cancer screenings, doctors may reject AI results due to a lack of transparency in their decisions. Deep neural networks also lack robustness and transparency, compromising security, and AI applications face risks such as data leakage and misuse, and strong regulatory and ethical rules are needed to ensure fairness and safety.[6]

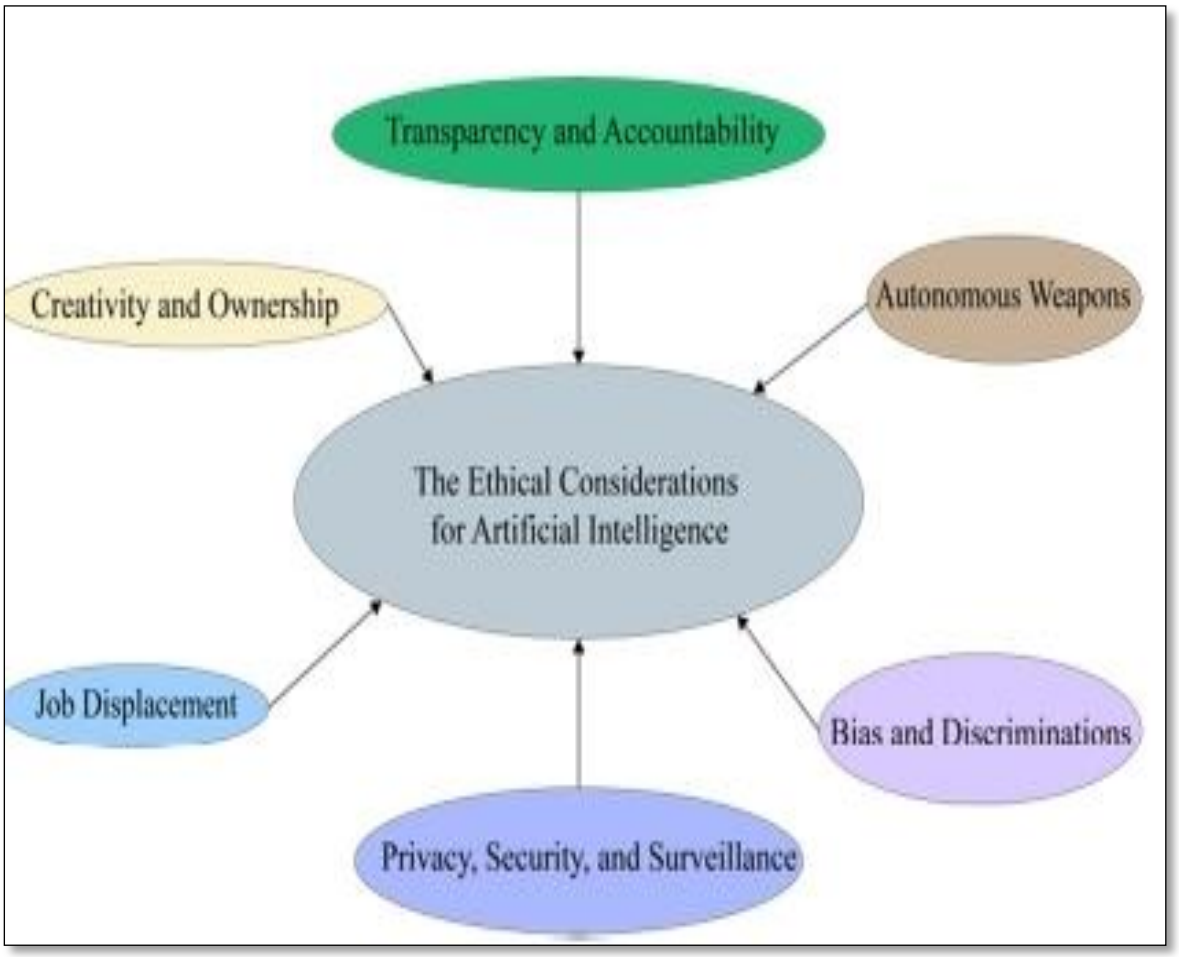

Figure 1. Ethical Challenges in AI.[6]

3.2. Bias in Algorithms

Bias in AI refers to bias in decision-making or recommendations by algorithmic models, resulting in unfair or discriminatory treatment of individuals or in machine learning models that discriminate against certain groups (often marginalized people based on race, gender, or social class). This bias can result from prior assumptions in model development or from inaccurate or unrepresentative training data. Bias can manifest in a number of ways, including historical bias from society, lack of diversity in the data, problems with measuring characteristics, and the use of inappropriate metrics, which can affect the fairness of the results. [8]

Also, the relationship between discrimination and bias in artificial intelligence and its impact on privacy is explained. [4]. Biased AI structures skilled on discriminatory data can also perpetuate systemic injustices via utilizing private details together with race, gender, religion, and political affiliations to make unjust choices. For instance, partial AI systems used for screening task applications may unfairly exclude applicants based on their gender or race, contributing to inequalities inside the workplace. Safeguards need to be implemented to guarantee that AI structures are trained on numerous and independent statistics assets to prevent discriminatory consequences.

Addressing bias in algorithm education records is critical for mitigating the dangers of unjust or discriminatory decisions within AI applications. By ensuring that training information is diverse and accountable, conducting bias tests earlier to use, and advocating for accountability and transparency in Artificial Intelligence decision-making strategies.

Table 1. Design of inquiries template for bias affects assertion [20]

What will the automated decision do?
Who is the audience for the algorithm and who will be most affected by it?
Do we have training data to make the correct predictions about the decision?
Is the training data sufficiently diverse and reliable? What is the data lifecycle of the algorithm?
Which groups are we worried about when it comes to training data errors, disparate treatment, and impact?
How will potential bias be detected?
How and when will the algorithm be tested? Who will be the targets for testing?
What will be the threshold for measuring and correcting for bias in the algorithm, especially as it relates to protected groups?
What are the operator incentives?
What will we gain in the development of the algorithm?
What are the potential bad outcomes and how will we know?
How open (e.g., in code or intent) will we make the design process of the algorithm to internal partners, clients, and customers?
What intervention will be taken if we predict that there might be bad outcomes associated with the development or deployment of the algorithm?
How are other stakeholders being engaged?
What's the feedback loop for the algorithm for developers, internal partners, and customers?
Is there a role for civil society organizations in the design of the algorithm?
Has diversity been considered in the design and execution?
Will the algorithm have implications for cultural groups and play out differently in cultural contexts?
Is the design team representative enough to capture these nuances and predict the application of the algorithm within different cultural contexts? If not, what steps are being taken to make these scenarios more salient and understandable to designers?
Given the algorithm's purpose, is the training data sufficiently diverse?
Are there statutory guardrails that companies should be reviewing to ensure that the algorithm is both legal and ethical?

Figure 2. Bias and Ethical Concerns in ML [12]

3.3. Security and Vulnerabilities

The introduction of AI generation has converted the landscape of information protection, bringing approximately superior equipment to discover and combat cyber threats successfully. Nevertheless, alongside the combination of AI and cybersecurity, a set of obstacles emerges, particularly concerning security vulnerabilities. [1] .Malicious

attacks on autonomous driving can cause vehicles to break traffic rules and cause accidents, highlighting the importance of strong privacy measures. Malicious data can distort AI models and influence drug recommendations in the medical sector. Despite the high accuracy of AI models in detecting cancer, doctors only agree on half of the results due to a lack of transparency. Deep neural networks lack transparency, which could result in felony and protection troubles. The use of massive information increases the threat of leakage and manipulation, and AI may be misused without oversight. Combining privacy and transparency is essential for the improvement of responsible AI. [6].

The usage of AI in cyberattacks and the emergence of the latest vulnerabilities underscore the importance of enforcing resilient security measures and vigilant tracking mechanisms. By proactively addressing those challenges, organizations can harness the entire capability of AI in cybersecurity while upholding moral requirements and ensuring transparency and responsibility ([1], [4], [9], [7]).

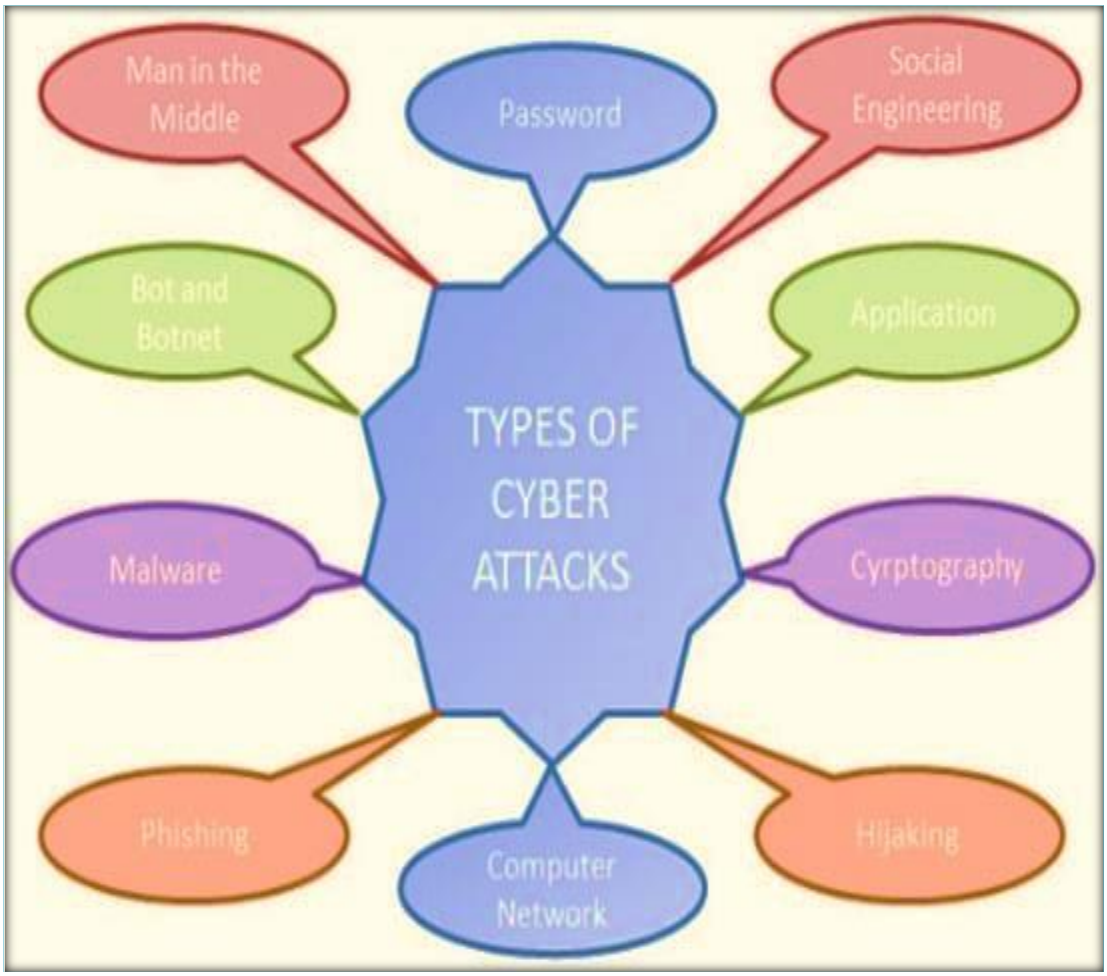

Figure 3. Common types of attacks [28]

3.4 Transparency and Accountability

Transparency and Accountability are key elements within the decision-making technique of synthetic intelligence (AI), especially within the realm of statistics protection. The significance of transparency lies in the capacity to understand the selection-making procedure of AI algorithms, which in the long run fosters trust and confidence within the gadget ([3]). Without transparency, users may also struggle to apprehend the inner workings of the structures they have interacted with, making it tough to hold accountable parties answerable for any ensuing outcomes ([17]. One of the number one hurdles concerning transparency with AI algorithms is their inherent complexity and absence of readability ([3]). Deep studying systems, upon which many AI algorithms are built, are in particular elaborate because of their interconnected nodes stimulated by neural networks ([17]. Transparency and

accountability are essential to the ethical considerations of AI systems, particularly with regard to minimizing bias. As AI becomes more integrated into society, fair and responsible application becomes essential. Artificial Intelligence systems can reflect biases present in the data used to train them. For example, a recruitment tool developed by Amazon using machine learning algorithms to screen resumes showed bias against women [10].

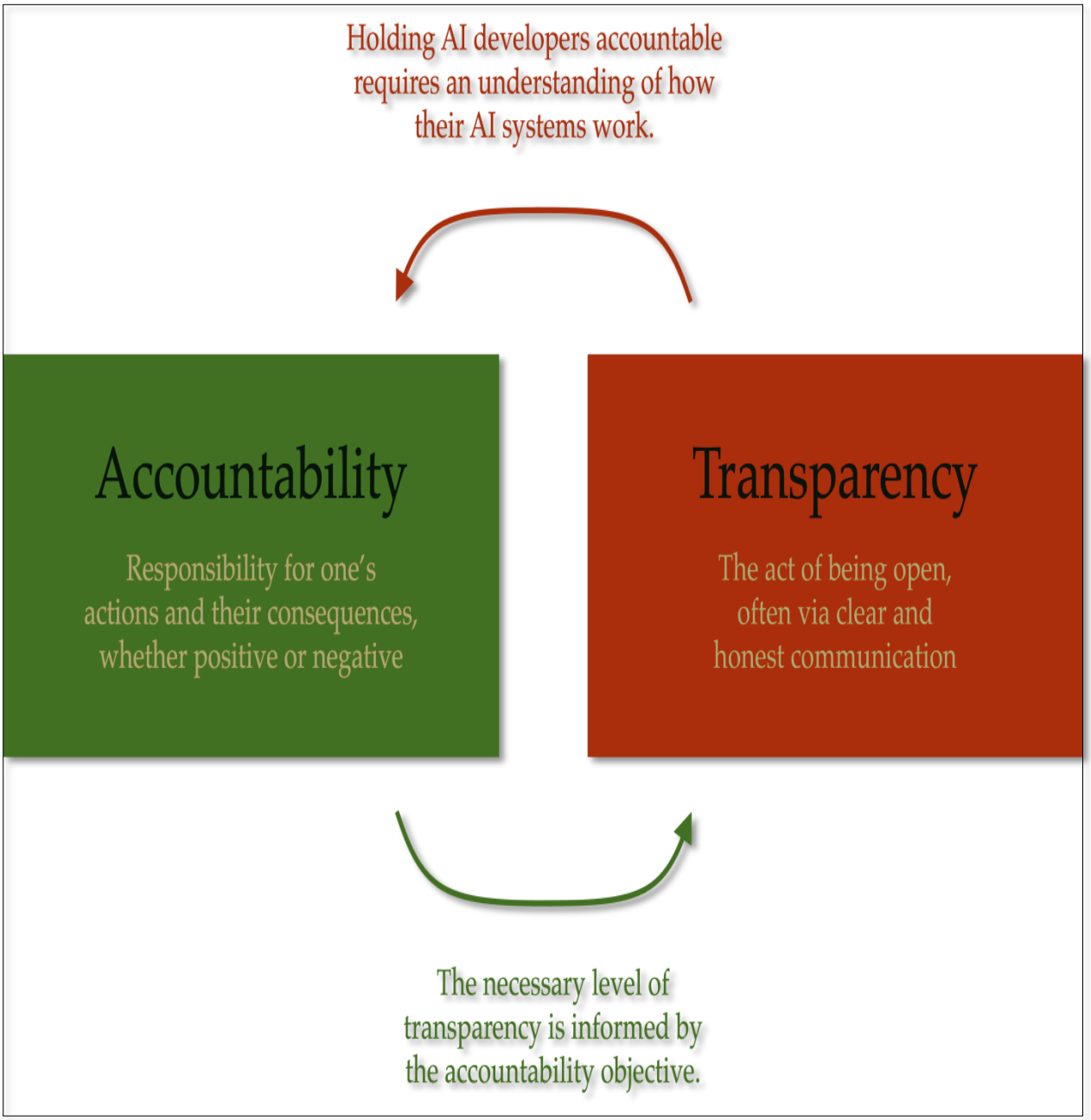

Figure 4. Accountability and Transparency in AI [29]

4. Case Studies on Ethical Dilemmas in AI Applicatipns

Ethical challenges arising from the use of AI in integration with other systems, such as gender and racial bias, must be addressed to avoid its negative effects on society. AI has the ability to distinguish between phenomena, such as distinguishing between healthy cells and cancer cells. In addition to protecting privacy. This requires legal and transparent processing. Transparency is challenged by companies seeking to obtain and monetize data, and the ethical challenges are not focused on AI but on how it is used and the consequences [25].

Table 2. Artificial intelligence application examples and problems it caused [23]

AI applications have raised legal issues around liability, requiring changes to the laws.	Traffic Application Examples and Legal Issues	Legal issues caused by automatic driving	Self-driving cars represent a major technological advance and are growing in popularity in China, but legal challenges such as determining liability in accidents must be addressed before they become widespread.
		Legal issues caused by smart trip planning	Navigation systems have evolved to become more accurate and easier, but the application of artificial intelligence has created security issues and legal liability that require intervention to protect users' rights.
	Application examples and legal issues in the medical field	he legal problems caused by surgical robots	Surgical robots are used to achieve better outcomes in operations, but they require human guidance. As technology advances, they may be able to perform operations autonomously, raising questions about risk and liability if errors occur.
		Legal issues caused by intelligent medical diagnosis	Smart robots are rapidly gaining medical knowledge and can accurately diagnose conditions, but there is a large gap between developing and developed countries, and the problem of liability for medical errors remains a legal challenge.
	Application Examples and Legal Issues in the Financial Sector	legal issues arising from smart stock operations	AI has become popular in stock trading to improve accuracy and stability, but profitable results vary depending on the design of the system, and irresponsible use can lead to significant market volatility, calling for regulation to avoid risks.
		Legal issues raised by smart investment consultants	Smart investment advisors provide personalized advice to investors and have developed rapidly in China. As no.of service providers increases, there is a need to regulate the sector to ensure qualifications of advisors and protect investors' rights from fraud.
	Business Application-s and Legal Issues	Legal issues raised by smart goods recommendat-ion	At the Double11 shopping festival, AI technologies have improved the shopping experience and transaction efficiency, but there are concerns about the liability of recommendation systems when promoting counterfeit goods, calling for consideration of ethical issues in e-commerce.
		Smart search triggered legal issues	Smart search engines combine AI and traditional techniques to provide personalized results to users. However, their economic relationship with merchants raises concerns about their impact on search results, which could lead to unfair practices.
	Security Application Examples and Legal Issues	Smart identification raises legal issues	AI technologies are used to recognize fingerprints, faces, and voices to enhance security, but there are risks related to protecting personal information, which calls for searching for ways to protect privacy.
	Security Application Examples and Legal Issues	Smart home induced legal issues	The smart home combines multiple technologies to enhance security and provide convenient services, but the use of these devices raises concerns about privacy, which calls for thinking about responsibility and addressing these issues.

5. Regulations and Guidelines for Ethical AI Use

Countries just like the UK and Austria have taken proactive measures to address the ethical dilemmas related to AI. For example, the establishment of a 'Centre for Data Ethics and Innovation' (CDEI) in the UK demonstrates a dedication to ensuring the ethical and stable usage of AI using evaluating dangers, analyzing regulatory frameworks, and providing steerage on first-class practices. Similarly, Austria's formation of a 'Robot Council' highlights the importance of promoting responsible AI usage, mitigating dangers, safeguarding records integrity, and encouraging public discourse [17].

Global initiatives together with the G7 Common Vision for the Future of AI ([17] underscore standards that propose human-centric AI, aid staff training and re-skilling, facilitate dialogue among multiple stakeholders to build consideration in AI innovations and sell investments in AI. These concepts underscore the need for ethical recommendations to control the improvement and deployment of AI technologies.

From a criminal point of view, [11] challenges the idea of inherent conflicts between the General Data Protection Regulation (GDPR) and AI. It shows that revolutionary policy options can be explored to promote responsible innovation without compromising information protection concepts. Moreover, [11] stresses that GDPR does not necessitate main changes to AI programs even emphasizing the significance of imparting steering to controllers and facts topics on aligning AI practices with GDPR.

6. Future Trends and Implications for Information Security

AI plays a major role in enhancing security against advanced threats. Its integration with blockchain technology, which provides strong data protection due to its decentralized and immutable nature, enables fraud detection and smart contract payment. Its integration with technologies such as quantum computing is expected to make traditional encryption algorithms more resistant to threats, and enhance real-time threat detection by accelerating big data processing. [16] Its integration with the IOTs, a promising future technology, is expected to connect billions of devices. Increased communications generate large amounts of data, and it is essential to keep that data safe from danger. [18] AI integration with IoT devices enhances security by continuously monitoring and adapting device behavior, encrypting and protecting data from hacking. [16]. Encryption is important to protect against unwanted access by the user. It is essential to provide privacy and security to users. It is used in medical systems, business, military, industrial, and multimedia. [18] In addition, continuous collaboration and learning with human experts will enable smarter systems to respond automatically to threats, contributing to enhanced security in the future. [16]

7. Conclusion

Artificial Intelligence has a significant impact on information security, improving the ability to detect security threats and responding to attacks. However, there are ethical dilemmas associated with this technology, such as protecting personal privacy from risks due to the complexity of the environment in which modern technology relies. AI technologies such as blockchain, encryption, the Internet of Things, and quantum computing are being integrated to preserve data and enhance information security in the future. Another dilemma is unintended algorithmic bias, which can lead to unfair outcomes by favoring one group over another, so the risk of unintended algorithmic bias in the work of Artificial Intelligence algorithms must be reduced in order to achieve justice and protect individual rights. Transparency and accountability must also be used to enhance security and maintain ethical standards.

Acknowledgements

The authors thank the College of Information Technology, University of Babylon for their continuous support and guidance during this research.

References

1. R. Rodrigues, "Legal and human rights issues of AI: Gaps, challenges and vulnerabilities", Journal of Responsible Technology,vol. 4, pp.1-36,Dec. 2020. [Online]. Available: https://doi.org/10.1016/j.jrt.2020.100005
2. A. Mughal. "Artificial Intelligence in Information Security: Exploring the Advantages, Challenges, and Future Directions", Journal of Artificial Intelligence and Machine Learning in Management, vol.2,no1,pp.22-34,Jan .2018. [Online]. Available: https://journals.sagescience.org/index.php/jamm/article/view/51
3. A. Limaj. "Ethical Considerations in AI-Powered Cybersecurity". Feb 2023. [Online]. Available: https://medium.com/@besniklimaj/ethical-considerations-in-ai-powered-cybersecurity-45cd83db90e0
4. M. Rijmenam. "Privacy in the Age of AI: Risks, Challenges and Solutions". Feb 2023. [Online]. Available: https://www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/
5. M. Jeyaraman, S. Balaji, N. Jeyaraman and S. Yadav. "Unraveling the Ethical Enigma: Artificial Intelligence in Healthcare". vol.15, no8,pp.1-6,Aug. 2023. [Online]. Available: DOI: 10.7759/cureus.43262
6. Li, N. ,"Ethical Considerations in Artificial Intelligence: A Comprehensive Disccusion from the Perspective of Computer Vision", In SHS Web of Conferences , SHS Web of Conferences 179, 04024, pp1-7,2023. [Online]. Available: https://doi.org/10.1051/shsconf/202317904024.

7. S.Kraus ,"Ethical Implementation of AI in Cybersecurity", (accessed Aug 03, 2024), [Online]. Available: https://www.evolvesecurity.com/blog-posts/ethical-implementation-of-ai-in-cybersecurity
8. L.Belenguer, "AI bias: exploring discriminatory algorithmic decision-making models and the application of possible machine-centric solutions adapted from the pharmaceutical industry. AI and Ethics", vol.2, no4, pp.771-787, Feb.
9. 2022. [Online]. Available: https:// doi: 10.1007/s43681-022-00138-8.
10. D. Humphreys, A. Koay, D. Desmond and E. Mealy. "AI hype as a cyber security risk: the moral responsibility of implementing generative AI in business". vol. 4, pp. 791–804, Feb 2024. [Online]. Available: https://link.springer.com/article/10.1007/s43681-024-00443-4
11. G. Mensah, "Artificial intelligence and ethics: a comprehensive review of bias mitigation, transparency, and accountability in AI Systems". Preprint, pp.1-26, Nov. 2023 . [Online]. Available: https://doi.10.13140/RG.2.2.23381.19685/1.
12. P. Sartor, D. Lagioia, "The impact of the General Data Protection Regulation (GDPR) on artificial intelligence", ISBN: 978-92-846-6771-0, pp.1-100 Jun. 2020. [Online]. Available: https:// doi.10.2861/293
13. N. Sutaria,"Bias and Ethical Concerns in Machine Learning", Aug.2022 [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-4/bias-and-ethical-concerns-in-machine-learning
14. M. Sullivan, "Examining Privacy Risks in AI Systems", Dec 2023. [Online]. Available: https://transcend.io/blog/ai-and-privacy
15. O.Akinrinola, C. Okoye, O. Ofodile, C. Ugochukwu, "Navigating and reviewing ethical dilemmas in AI development: Strategies for transparency, fairness, and accountability". GSC Advanced Research and Reviews, vol.18,no.3, pp.050-058.2024. [Online]. Available: https://doi.org/10.30574/gscarr.2024.18.3.0088.
16. P.Detopoulou, G.Voulgaridou, P.Moschos, D.Levidi, T.Anastasiou, V. Dedes, S. Papadopoulou, "Artificial intelligence, nutrition, and ethical issues: A mini-review". Clinical Nutrition Open Science.223, vol. 50,pp.46-56,Aug. 2023. [Online]. Available: https://doi.org/10.1016/j.nutos.2023.07.001
17. K.Ramachandran, "The Role of Artificial Intelligence in Enhancing financial Data Security", Journal ID: 4867, 9994. 2024., IJAIAP, vol.3,no. 1, pp.1-13. [Online]. Available:
18. https://iaeme.com/masteradmin/journal_uploads/ijaiap/volume_3_issue_1/ijaiap_03_01_001.pdf
19. E. Bird, J. Fox-Skelly, N. Jenner, R. Larbey, E. Weitkamp, A. Winfield. "The ethics of artificial intelligence: Issues and initiatives". ISBN: 978-92-846-5799-5, pp.1-113, Mar. 2020, [Online]. Available: https:// doi: 10.2861/6644
20. S. Hussein, A. Hamza, S.Al-Shoukry , M. Zahra, S.Nouwar, S. Abdulkareem, , M. Jaber, "Evaluating Image Encryption Algorithms for The Hyperchaotic System and Fibonacci Q-Matrix, Secure Internet of Things, and Advanced Encryption Standard". Eastern-European Journal of Enterprise Technologies, vol.19, no.2, Nov.2022. [Online]. Available: https:// 10.15587/1729-4061.2022.265862
21. G.Karimian, E.Petelos,S. Evers,"The ethical issues of the application of artificial intelligence in healthcare: a systematic scoping review". AI and Ethics, vol.2, no .4, pp.539-551, Mar.2022. [Online]. Available:
22. https://doi.org/10.1007/s43681-021-00131-7
23. N. Turner, " Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms". May.2019. [Online]. Available: https://www.brookings.edu/articles/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/
24. A. Banga,"Impact of artificial intelligence on cyber security", International Journal For Technological Research In Engineering, vol.11, no .4,pp. 61-64,Dec.2023. [Online]. Available:
25. https://www.researchgate.net/publication/377231405_impact_of_artificial_intelligence_on_cyber_security#fullTextFileContent
26. A. Hamza, & S. M. Al-Alak, "Study of environmentally sustainable security in wireless sensor networks", Periodicals of Engineering and Natural Sciences, vol.7, no .4, pp. 1722-1732, Dec.2019. [Online]. Available:
27. DOI: http://dx.doi.org/10.21533/pen.v7i4.915
28. L..Ma, Z.Zhang, N.Zhang, "Ethical dilemma of artificial intelligence and its research progress". In IOP conference series: materials science and engineering 392 (2018) 062188, pp.1-4, Jul.2018. [Online]. Available: doi:10.1088/1757-899X/392/6/062188
29. O. Farayola, O. Olorunfemi, P. Shoetan, "Data privacy and security in it: a review of techniques and challenges. Computer Science & IT Research Journal, vol.5, no.3, pp.606-615, Mar.2024. [Online]. Available: doi: https://doi.org/10.51594/csitrj.v5i3.909

30. B. Stahl, D. Schroeder, R.Rodrigues, "Ethics of artificial intelligence: case studies and options for addressing ethical challenges, Springer Nature, ISBN 978-3-031-17039-3, pp.1- 116,2023. [Online]. Available: https://library.oapen.org/bitstream/handle/20.500.12657/59315/978-3-031-17040-9.pdf?sequence=1
31. M. Team. "Safeguarding Digital Frontiers Through AI In Cybersecurity" July.2024. [Online]. Available:
32. https://www.axcelerate.ai/blog/f498ac4c-e195-4f9b-a48b-4c7e13518b88
33. M. Binhammad, S. Alqaydi, A. Othman, L. Abuljadayel," The Role of AI in Cyber Security: Safeguarding Digital Identity", Journal of Information Security, vol.15, no.2, Apr.2024. [Online]. Available: https://10.4236/jis.2024.152015
34. L.Yuchong, L.Qinghui ,"A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics", Vol. 7, pp. 8176-8186,2021, Nov. 2021. [Online]. Available: https://doi.org/10.1016/j.egyr.2021.08.126
35. J. SIDERIUS, C. SARAH, C. FABRIZIO, "Introduction to AI Accountability & Transparency Series", SEP. 2023. [Online]. Available: https://aipolicy.substack.com/p/ai-accountability-transparency-intro