International Journal of Research in Economics and Social Sciences(IJRESS)
Available online at: http://euroasiapub.org
Vol. 14 Issue 05 May- 2024
ISSN: 2249-7382 | Impact Factor: 8.018|
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

The Era of Artificial intelligence Deep Fake and Privacy Vulnerabilities

Author: Avneet Minhas, Faculty of Law, University Institute of Legal Studies, Panjab University, Chandigarh

Email:- avneetminhas91@gmail.com

Co-author: Dr. Amita Arora, Faculty of Law, University Institute of Legal studies, Panjab University, Chandigarh

Email:-Amyamita98@gmail.com

Abstract

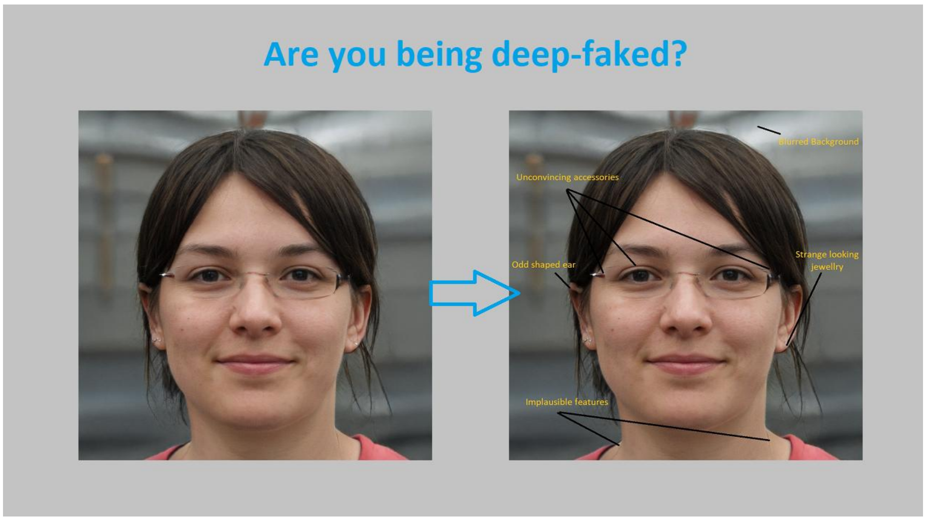
The rise of artificial intelligence (AI) has led to a proliferation of deep fake technology, raising significant concerns about privacy vulnerabilities. Deep fake algorithms can generate highly realistic but fabricated images, audio, and videos, blurring the lines between truth and fiction. This poses serious threats to individuals' privacy, as malicious actors can exploit these tools to manipulate or fabricate sensitive content, such as fake news or compromising videos. Moreover, the widespread availability of deep fake technology amplifies the potential for misinformation and social engineering attacks, undermining trust in digital media and exacerbating societal divisions. As AI continues to advance, addressing the ethical and legal implications of deep fake technology is paramount to safeguarding privacy rights and preserving the integrity of digital content. Efforts to develop robust detection methods and regulatory frameworks are essential to mitigate the risks posed by deep fakes and protect individuals from privacy violations in the digital age.

Keywords:- *Artificial Intelligence, Deep fake, Privacy vulnerabilities, Digital manipulation*

Introduction

Artificial intelligence (AI) has revolutionized various aspects of technology, communication, and media. However, alongside the advancements in AI, a concerning trend has arisen: the proliferation of deep fake technology. Deep fakes refer to highly sophisticated AI-generated content, including images, videos, and audio recordings, that are manipulated or entirely fabricated to appear authentic. This technological advancement has ushered in a new era fraught with privacy vulnerabilities and ethical dilemmas.The exponential growth of deep fake technology poses a significant threat to privacy rights and digital integrity. By leveraging AI algorithms, deep fake creators can produce hyper-realistic simulations of individuals, enabling the fabrication of convincing yet entirely false narratives. These manipulated media can range from impersonations of public figures to falsified evidence in legal proceedings, blurring the distinction between fact and fiction. Consequently, the proliferation of deep fakes has heightened concerns surrounding privacy violations and misinformation in the digital sphere.

The accessibility of deep fake tools and platforms exacerbates the potential for malicious exploitation. With minimal technical expertise, individuals can create and disseminate deceptive content with ease, amplifying the risk of social engineering attacks and online harassment. Furthermore, the anonymity afforded by the internet enables bad actors to exploit deep fakes for extortion, defamation, and political manipulation, undermining trust in digital media and democratic institutions.As deep fake technology continues to evolve, addressing its ethical, legal, and societal implications becomes imperative. Effective strategies must be implemented to mitigate the risks associated with deep fakes, safeguard individuals' privacy, and preserve the integrity of digital content. This necessitates interdisciplinary collaboration among technologists, policymakers, and ethicists to develop robust detection mechanisms, regulatory frameworks, and public awareness campaigns to combat the growing threat of deep fake-induced privacy vulnerabilities.



In India, victims of deepfake incidents have legal avenues for recourse. Social media platforms are obligated to address complaints related to cybercrime and promptly remove deepfake content within 36 hours. Victims can report cybercrime incidents to the National Cyber Crime Helpline (1930) and enlist the support of a cyber lawyer[1].

The legal framework governing deepfake offenses in India includes Section 66 of the Information Technology Act, 2000, which addresses cybercrime offenses such as counterfeiting and dissemination of false information. Furthermore, under the Copyright Act of 1957, deepfakes may breach copyright laws if they involve the unauthorized use of copyrighted material.

In addition to these statutes, provisions of the Indian Penal Code (IPC) come into play. For instance, defamation (Section 499) and criminal intimidation (Section 506) can be invoked depending on the nature of the deepfake incident. These legal remedies provide victims with avenues to seek justice and protection against the harmful effects of deepfake manipulation.

Overview of Deep Fake Technology

Deep fake technology refers to the use of artificial intelligence (AI) algorithms to create highly convincing but entirely fabricated media, including images, videos, and audio recordings. This innovative technology enables the manipulation of digital content to such an extent that it becomes increasingly challenging to discern between real and fake media.At the core of deep fake technology are generative adversarial networks (GANs) and deep learning techniques, which allow for the synthesis of hyper-realistic content by analyzing and mimicking patterns from large datasets. By leveraging these advanced algorithms, users can seamlessly superimpose faces onto bodies, manipulate facial expressions and gestures, and even alter voices with remarkable accuracy.The applications of deep fake technology are diverse and range from entertainment and artistic expression to more nefarious purposes such as political manipulation, misinformation, and online harassment. While deep fake technology has the potential to revolutionize various industries, its proliferation also poses significant ethical, legal, and societal challenges.As deep fake technology continues to evolve and become

[1] Taddeo, M., McCutcheon, T., &Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. Nature Machine Intelligence, 1(12), 557-560.

increasingly accessible, there is a growing need for robust detection methods, regulatory frameworks, and public awareness initiatives to mitigate the risks associated with its misuse and safeguard the integrity of digital content.

Real-world applications and implications

Deep fake technology has found its initial prominence in the entertainment sector, particularly for tasks like seamlessly swapping faces in movies and crafting lifelike CGI characters.the technology's application extends beyond entertainment and has been exploited for nefarious purposes in various domains:In politics and misinformation, deep fake technology has been utilized to craft deceptive political content, manipulate speeches, and propagate false narratives. This misuse poses a significant threat to democratic processes and undermines public trust in information dissemination.deep fakes have raised concerns in the realm of fraud and cybersecurity, where they can facilitate activities such as voice phishing and the creation of convincing fake identities for cybercrimes. This presents challenges regarding the vulnerability of individuals and organizations to identity theft and financial fraud.In the study of social media and influencer culture, deep fake technology introduces uncertainties about the authenticity of content attributed to influencers and celebrities. This uncertainty can affect their reputation and erode trust among their followers.As deep fake technology continues to evolve, it is crucial to address these multifaceted challenges through robust detection mechanisms, regulatory frameworks, and public awareness initiatives to mitigate the risks associated with its misuse and protect individuals' privacy and digital integrity[2].

Need of the Study

The proliferation of deep fake technology in the era of artificial intelligence has raised significant concerns regarding privacy vulnerabilities and ethical implications. However, there remains a gap in understanding the specific impacts of deep fakes on individuals' privacy rights and digital integrity. This study aims to address this gap by examining the prevalence of deep fake creation, dissemination, and the potential consequences for privacy violations. By

[2] Fletcher, J. (2018). Deepfakes, Artificial Intelligence, and Some Kind of Dystopia. Theatre Journal, 70(4), 455-471.

investigating the perceptions, experiences, and concerns of individuals regarding deep fakes, this research seeks to provide valuable insights into the urgent need for regulatory measures, detection mechanisms, and public awareness campaigns to mitigate the risks posed by deep fake technology. Ultimately, the findings of this study aim to inform policymakers, technologists, and the public about the critical importance of safeguarding privacy rights and preserving the integrity of digital media in the face of advancing AI technology.

Literature Review

Manheim, K., & Kaplan, L. (2019). Artificial intelligence (AI) presents significant risks to both privacy and democracy. AI systems, particularly those fueled by vast amounts of personal data, can lead to pervasive surveillance and erosion of privacy rights. As AI algorithms analyze and predict individual behaviors, concerns arise regarding the potential for manipulation and exploitation of personal information by governments and corporations. Moreover, AI-powered decision-making processes may exacerbate inequalities and biases, leading to discriminatory outcomes in areas such as employment, housing, and criminal justice. In democratic contexts, the concentration of AI power in the hands of a few entities could undermine transparency and accountability, threatening the principles of open governance and citizen participation. Safeguarding privacy and democracy in the age of AI requires robust regulatory frameworks, ethical guidelines, and public awareness campaigns to mitigate risks and ensure that AI technologies are developed and deployed responsibly for the benefit of society[3].

Liu, X., Xie, L., Wang, et al (2020). Privacy and security concerns are paramount in the domain of deep learning, as the technology relies heavily on vast datasets, often containing sensitive personal information. Deep learning models, particularly when trained on large-scale datasets, may inadvertently capture and retain sensitive user data, raising risks of unauthorized access, misuse, or breaches. Moreover, the opaque nature of deep learning algorithms makes it challenging to understand how they process and utilize data, exacerbating privacy risks. Adversarial attacks, where malicious actors manipulate inputs to deceive deep learning systems, pose further security threats, potentially leading to incorrect or harmful outcomes.

[3] Manheim, K., & Kaplan, L. (2019). Artificial intelligence: Risks to privacy and democracy. Yale JL & Tech., 21, 106

Chesney, B., & Citron, D. (2019). Deepfakes, synthetic media generated by deep learning algorithms, pose a significant and multifaceted threat to privacy, democracy, and national security. These hyper-realistic videos and audio recordings can be manipulated to depict individuals saying or doing things they never did, leading to misinformation, defamation, and even blackmail. In the realm of privacy, deepfakes can undermine trust and integrity, as individuals' identities can be falsely portrayed without their consent. In democracies, the spread of deepfakes can erode public trust in institutions and sow confusion during elections or other critical events[4].

Brundage, M., Avin, et al (2018). The malicious use of artificial intelligence (AI) presents a growing concern, as advancements in AI technology offer new capabilities for malicious actors to exploit. Forecasting, preventing, and mitigating such threats require a multifaceted approach. Proactive measures include developing robust AI-driven threat detection systems that can anticipate and identify potential malicious activities. promoting responsible AI development through ethical guidelines and regulatory frameworks can mitigate risks associated with the misuse of AI. Collaboration between governments, industry, academia, and civil society is essential to share information, resources, and best practices for combating AI-driven threats effectively.

Fletcher, J. (2018). The proliferation of deepfakes, driven by advancements in artificial intelligence, raises concerns about the potential emergence of a dystopian reality. Deepfakes, which use AI algorithms to create convincingly realistic fake videos and audio recordings, have the capacity to manipulate public perception, sow discord, and undermine trust in information and institutions. In this dystopian scenario, individuals and societies may find themselves unable to discern truth from fiction, leading to widespread confusion and disorientation. The malicious use of deepfakes could also exacerbate existing societal divisions, amplify political polarization, and erode democratic norms[5].

Taddeo, M., McCutcheon, et al (2019). Trusting artificial intelligence (AI) in cybersecurity presents a double-edged sword dilemma. On one hand, AI-powered cybersecurity solutions

[4] Chesney, B., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. Calif. L. Rev., 107, 1753.

[5] Fletcher, J. (2018). Deepfakes, Artificial Intelligence, and Some Kind of Dystopia. Theatre Journal, 70(4), 455-471.

offer the promise of faster threat detection, more accurate risk assessment, and proactive defense mechanisms. These systems can analyze vast amounts of data in real-time, identify patterns indicative of cyber threats, and respond swiftly to mitigate potential breaches. However, relying solely on AI for cybersecurity also poses significant risks.

Bécue, A., Praça, I., & Gama, J. (2021). In the era of Industry 4.0, the integration of artificial intelligence (AI) brings forth both challenges and opportunities in cybersecurity. While AI technologies offer immense potential for optimizing operations and enhancing productivity in various industries, they also introduce new cyber-threats. These threats range from sophisticated cyber-attacks leveraging AI algorithms to manipulate data and infiltrate systems to the exploitation of AI vulnerabilities for malicious purposes. Consequently, safeguarding critical infrastructure and sensitive data becomes paramount.

Cheatham, B., Javanmardian, K., et al (2019). Confronting the risks of artificial intelligence (AI) involves addressing various concerns regarding its ethical, societal, and technical implications. Ethical considerations include ensuring transparency, accountability, and fairness in AI systems to prevent biases and discriminatory outcomes. safeguarding privacy and data security is crucial, especially with the potential for AI to exacerbate surveillance and infringe on individual rights. Societal risks encompass job displacement due to automation, exacerbating inequality, and the misuse of AI for malicious purposes such as disinformation campaigns or autonomous weapons. From a technical perspective, challenges include ensuring AI systems are robust, reliable, and resilient to adversarial attacks or unintended consequences[6].

Zeadally, S., Adi, E., et al (2020). Harnessing artificial intelligence (AI) capabilities presents a promising avenue for bolstering cybersecurity defenses in an increasingly digital world. AI technologies can analyze vast amounts of data at incredible speeds, enabling proactive threat detection and rapid response to cyberattacks. Machine learning algorithms can identify patterns indicative of malicious activity, allowing for the early detection of emerging threats. Moreover,

[6] Cheatham, B., Javanmardian, K., &Samandari, H. (2019). Confronting the risks of artificial intelligence. McKinsey Quarterly, 2(38), 1-9.

AI-powered systems can autonomously adapt and evolve to counter evolving cyber threats in real-time, reducing the burden on human analysts and enhancing overall cybersecurity posture[7].

Liu, B., Ding, M., Shaham, S. et al (2021). As machine learning (ML) continues to proliferate across various domains, the intersection of ML and privacy has become a critical area of concern. The widespread adoption of ML algorithms often entails the collection and analysis of vast amounts of personal data, raising significant privacy implications. Researchers and practitioners are increasingly exploring techniques to reconcile the benefits of ML with individual privacy rights. This includes developing privacy-preserving ML algorithms that operate on encrypted data or employ anonymization techniques to prevent the disclosure of sensitive information. Additionally, frameworks such as differential privacy aim to provide strong privacy guarantees by injecting noise into data or query responses while still enabling meaningful analysis.

Significance of the Study

1. Impact on personal privacy

The pervasive utilization of deep fake technology elicits profound apprehensions regarding personal privacy. It exposes individuals to the threat of exploitation by nefarious entities who employ deep fakes to construct deceitful narratives or fabricate compromising scenarios. Consequently, the risk of detrimental consequences to an individual's reputation and psychological welfare is considerable. Such manipulation not only undermines the trustworthiness of digital media but also amplifies the vulnerability of individuals to exploitation and harm. As deep fake technology continues to advance, the imperative to safeguard personal privacy becomes increasingly urgent, necessitating robust measures to counteract its misuse and mitigate the potential adverse impacts on individuals and society as a whole.

2. Influence on public perception and trust

The widespread dissemination of deep fakes carries the capacity to undermine public trust and confidence in the authenticity of digital content. When individuals struggle to differentiate

[7] Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. Ieee Access, 8, 23817-23837.

between genuine and manipulated media, it can precipitate a breakdown in trust across various domains, including institutions, public figures, and interpersonal relationships. This erosion of trust can have far-reaching consequences, affecting societal cohesion, democratic processes, and individual well-being. As deep fake technology continues to advance, the need for effective measures to combat its proliferation becomes increasingly urgent. Safeguarding the integrity of digital content is essential to preserving trust in the digital age and upholding the credibility of information dissemination channels. Therefore, concerted efforts are required from policymakers, technology developers, and the broader community to mitigate the harmful effects of deep fakes and maintain trust in digital media[8].

3. Need for a legal framework

Considering the potential harms linked with deep fake technology, there exists an urgent necessity for a robust legal framework to govern its usage. Such a framework should encompass regulations concerning the creation, dissemination, and malicious exploitation of deep fakes. However, striking a balance between safeguarding personal privacy and permitting the legitimate application of innovative technologies presents a formidable challenge.A comprehensive legal framework would need to delineate clear guidelines for the creation and sharing of deep fake content, ensuring accountability and liability for those who misuse the technology for harmful purposes. Simultaneously, it should safeguard individuals' rights to privacy and protect them from the detrimental effects of manipulated media.the legal framework should incorporate mechanisms for swift detection and removal of deep fake content from digital platforms, along with provisions for redressal and compensation for victims of deep fake manipulation.

Privacy Laws in India

Existing legal framework for privacy

India's legal framework for privacy is in a state of development and has undergone significant evolution over time. The right to privacy is now firmly established as a fundamental right under the Indian Constitution, a milestone reaffirmed by the Supreme Court of India in its landmark

[8] Hamon, R., Junklewitz, H., & Sanchez, I. (2020). Robustness and explainability of artificial intelligence. Publications Office of the European Union, 207.

ruling in the case of Justice K. S. Puttaswamy (Retd.) vs. Union of India in 2017. In this pivotal judgment, the court unequivocally declared privacy to be an intrinsic component of the right to life and personal liberty enshrined in Article 21 of the Constitution. This ruling marked a significant turning point in India's legal landscape, providing a strong foundation for the protection of individual privacy rights. Since then, the Indian legal system has continued to evolve, with ongoing efforts to develop and strengthen privacy laws and regulations to address the complexities of the digital age. As India navigates the challenges posed by technological advancements and the increasing digitalization of society, the protection of privacy rights remains a crucial priority in shaping the country's legal framework[9].

Key legislations (e.g., Information Technology Act, 2000)

One of the key legislations concerning privacy and digital rights in India is the Information Technology (IT) Act of 2000. This act was enacted to provide legal recognition for electronic transactions and facilitate e-governance by ensuring secure electronic communication and data exchange. It contains provisions related to data protection, cybersecurity, and digital signatures, among other things.Another important legislation is the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act of 2016. This act establishes the legal framework for the Aadhaar biometric identity system, which assigns a unique identification number to Indian residents. While the Aadhaar system aims to streamline access to government services and subsidies, concerns have been raised about its implications for privacy and data security.the Right to Information Act of 2005 empowers citizens to access information held by public authorities, promoting transparency and accountability in government functioning. However, there are ongoing debates about the balance between transparency and privacy rights under this legislation. These key legislations collectively shape the legal landscape for privacy and digital rights in India, influencing how individuals' personal data is managed and protected in the digital age.

Deep Fake Technology and Privacy Concerns

[9] Agarwal, V. (2012). Privacy and data protection laws in India. International Journal of Liability and Scientific Enquiry, 5(3-4), 205-212.

Deep fake technology, while innovative and intriguing, raises significant privacy concerns in today's digital landscape. This technology, which utilizes artificial intelligence to create highly convincing but entirely fabricated media, including images, videos, and audio recordings, poses a serious threat to individuals' privacy rights.One of the primary concerns is the potential for deep fakes to be used for malicious purposes, such as creating false narratives or fabricating compromising situations involving individuals without their consent. This can lead to reputational harm, emotional distress, and even financial or personal safety risks for the victims of deep fake manipulation.deep fakes blur the line between truth and fiction, making it increasingly difficult for individuals to discern authentic content from manipulated media. This erosion of trust in digital media undermines the integrity of information dissemination channels and poses challenges for maintaining public discourse and democratic processes.the widespread availability of deep fake technology raises concerns about the unauthorized use of individuals' likeness and voice, infringing on their right to control their personal image and identity[10].

These privacy concerns requires a multifaceted approach, including the development of robust detection mechanisms, regulatory frameworks, and public awareness campaigns. By taking proactive steps to mitigate the risks associated with deep fake technology, we can better protect individuals' privacy rights and preserve the integrity of digital content in the digital age.

Research Problem

The proliferation of artificial intelligence (AI)-generated deep fake technology has introduced profound privacy vulnerabilities in the digital landscape, presenting a critical research problem. Despite increasing awareness of deep fake technology, there remains a gap in understanding the extent of its impact on privacy and the efficacy of current mitigation strategies. This research problem encompasses several key considerations. Exploring the prevalent forms and sources of deep fake content circulating online is crucial. how individuals perceive and respond to the threat of deep fakes in terms of their privacy concerns is essential. Examining the potential legal and ethical implications of deep fake technology for privacy rights is necessary. Fourth, analyzing the limitations and challenges associated with existing detection and mitigation

[10] Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. Journal of Responsible Technology, 4, 100005.

approaches for deep fakes is vital. Identifying strategies to effectively mitigate the risks posed by deep fakes and safeguard individuals' privacy in the digital age is imperative. Addressing these considerations is essential to inform policy decisions, technological advancements, and public awareness efforts aimed at protecting privacy rights amidst the proliferation of AI-generated deep fake content.

Suggestion of the Study

Stopping deep fake technology entirely is challenging due to its complex nature and the rapid advancement of artificial intelligence. However, there are several strategies to mitigate its harmful effects:

1. **Legislation and Regulation:** Governments can enact laws and regulations specifically targeting deep fake creation, dissemination, and malicious use. These regulations can include penalties for creating or sharing deep fakes without consent or for malicious purposes.
2. **Platform Policies:** Social media platforms and content-sharing websites can implement policies to detect and remove deep fake content. They can also provide tools for users to report suspected deep fakes and educate users about the risks associated with manipulated media.
3. **Technological Solutions:** Researchers can develop technologies to detect and identify deep fakes, such as machine learning algorithms trained to recognize patterns indicative of manipulation. These tools can be integrated into digital platforms to automatically flag suspicious content.
4. **Media Literacy and Education:** Educating the public about the existence and potential dangers of deep fake technology can help individuals become more discerning consumers of digital content. Media literacy programs can teach people how to spot signs of manipulation and verify the authenticity of media they encounter online.
5. **Collaboration:** Collaboration between governments, tech companies, researchers, and civil society organizations is essential to effectively address the challenges posed by

deep fake technology. By working together, stakeholders can develop comprehensive strategies to combat deep fakes and protect individuals' privacy and digital integrity.

While it may not be possible to completely eradicate deep fake technology, implementing these strategies can help mitigate its harmful effects and safeguard individuals and societies from its negative impacts.

Conclusion

Deep fake technology in the era of artificial intelligence presents unprecedented challenges to privacy rights and digital integrity. The rapid advancements in AI algorithms have enabled the creation of highly convincing and deceptive media, blurring the lines between reality and fabrication. As demonstrated throughout this study, deep fakes pose significant risks to individuals' privacy, as malicious actors can exploit this technology for various nefarious purposes, including misinformation, social engineering, and defamation.the accessibility of deep fake tools amplifies the potential for widespread dissemination of manipulated content, undermining trust in digital media and democratic institutions. Despite growing awareness of the threats posed by deep fakes, effective strategies to combat this phenomenon remain elusive.Therefore, urgent action is needed to address the ethical, legal, and societal implications of deep fake technology. This includes the development of robust detection mechanisms, regulatory frameworks, and public education campaigns to mitigate the risks associated with deep fakes and safeguard individuals' privacy rights. Only through collaborative efforts among policymakers, technologists, and the public can we navigate the challenges posed by deep fakes and preserve the integrity of digital communication in the age of artificial intelligence.

References

1. Manheim, K., & Kaplan, L. (2019). Artificial intelligence: Risks to privacy and democracy. Yale JL & Tech., 21, 106
2. Liu, X., Xie, L., Wang, Y., Zou, J., Xiong, J., Ying, Z., &Vasilakos, A. V. (2020). Privacy and security issues in deep learning: A survey. IEEE Access, 9, 4566-4593..
3. Chesney, B., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. Calif. L. Rev., 107, 1753.

4. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ...&Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv preprint arXiv:1802.07228.
5. Fletcher, J. (2018). Deepfakes, Artificial Intelligence, and Some Kind of Dystopia. Theatre Journal, 70(4), 455-471.
6. Fletcher, J. (2018). Deepfakes, Artificial Intelligence, and Some Kind of Dystopia. Theatre Journal, 70(4), 455-471.
7. Taddeo, M., McCutcheon, T., &Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. Nature Machine Intelligence, 1(12), 557-560.
8. Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. Artificial Intelligence Review, 54(5), 3849-3886.
9. Cheatham, B., Javanmardian, K., &Samandari, H. (2019). Confronting the risks of artificial intelligence. McKinsey Quarterly, 2(38), 1-9.
10. Maras, M. H., &Alexandrou, A. (2019). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos. The International Journal of Evidence & Proof, 23(3), 255-262.
11. Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. Ieee Access, 8, 23817-23837.
12. Liu, B., Ding, M., Shaham, S., Rahayu, W., Farokhi, F., & Lin, Z. (2021). When machine learning meets privacy: A survey and outlook. ACM Computing Surveys (CSUR), 54(2), 1-36.
13. Mughal, A. A. (2018). Artificial Intelligence in Information Security: Exploring the Advantages, Challenges, and Future Directions. Journal of Artificial Intelligence and Machine Learning in Management, 2(1), 22-34.
14. Hamon, R., Junklewitz, H., & Sanchez, I. (2020). Robustness and explainability of artificial intelligence. Publications Office of the European Union, 207.
15. Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. Journal of Responsible Technology, 4, 100005.

16. Hao, M., Li, H., Luo, X., Xu, G., Yang, H., & Liu, S. (2019). Efficient and privacy-enhanced federated learning for industrial artificial intelligence. IEEE Transactions on Industrial Informatics, 16(10), 6532-6542.
17. Singh, S. K., Rathore, S., & Park, J. H. (2020). Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. Future Generation Computer Systems, 110, 721-743
18. Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., &Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. Electronics, 11(2), 198.
19. Tan, L., Yu, K., Ming, F., Cheng, X., & Srivastava, G. (2021). Secure and resilient artificial intelligence of things: a HoneyNet approach for threat detection and situational awareness. IEEE Consumer Electronics Magazine, 11(3), 69-78.
20. Mogaji, E., Soetan, T. O., &Kieu, T. A. (2020). The implications of artificial intelligence on the digital marketing of financial services to vulnerable customers. Australasian Marketing Journal, j-ausmj.

****