GAP iNTERDISCIPLINARITIES
A Global Journal of Interdisciplinary Studies
(ISSN – 2581-5628)
Impact Factor: SJIF - 5.363, IIFS - 4.875
Globally peer-reviewed and open access journal.

THE PUBLIC PERCEPTION OF IMPACT OF AI ON CYBERSECURITY

Dr. Ansari Mohd. Nasir *, Dr Bhagyashree Tamhane**

MCM, MBA, M.Phil,.Ph.D
(Asst. Prof. In Information Technology, K.P.B..Hinduja College of Commerce)

M.A ,Ph.D ,UGC-NET
(Librarian at K.P.B..Hinduja College of Commerce)

Abstract

This study explores the public perception of the impact of artificial intelligence (AI) on cybersecurity, focusing on how demographic factors such as age and gender influence individuals' views. The analysis reveals that while gender does not significantly affect trust or awareness of AI in cybersecurity, it does influence privacy concerns, with females expressing higher levels of worry. Age, however, has a more pronounced effect, with younger individuals showing greater trust, awareness, and concern about privacy related to AI technologies in cybersecurity. These findings highlight that younger generations are more receptive to AI-driven solutions but also more cautious about privacy implications. The results offer insights for policymakers and technology developers to create AI solutions that address public concerns and encourage wider adoption of AI in cybersecurity.

INTRODUCTION:

Artificial Intelligence (AI) has emerged as one of the most transformative technologies of the 21st century, reshaping industries, organizations, and societies at large. Its impact on cybersecurity, in particular, has become a subject of increasing importance and scrutiny. With the rise of cyber threats, including data breaches, ransomware attacks, and system vulnerabilities, AI has been presented as both a potential solution and a double-edged sword in the fight against cybercrime. As AI continues to evolve, it is imperative to examine the public perception of its role in cybersecurity, as it is the general public and businesses that bear the consequences of its application.

In recent years, AI-driven cybersecurity tools have gained popularity due to their ability to process and analyze vast amounts of data at speeds and accuracy levels unattainable by human efforts. AI algorithms, such as machine learning and deep learning, have been integrated into security systems to detect anomalies, predict threats, and automate responses to cyber-attacks. These systems are designed to enhance security measures and minimize human error, which is often exploited by cybercriminals. However, as the deployment of AI in cybersecurity grows, so does the concern regarding its potential risks and challenges, including privacy violations, biases in decision-making, and the replacement of human jobs.

While the technological benefits of AI in cybersecurity are widely recognized, there is a significant gap in understanding how the public perceives these advancements. Public perception plays a crucial role in the acceptance and implementation of new technologies, particularly in sensitive areas like cybersecurity. Public trust in AI systems is influenced by a variety of factors, such as understanding the technology, perceived risks, and the potential for AI systems to improve or disrupt cybersecurity practices. The way in which AI is integrated into everyday life, including personal devices, online banking, and government databases, further amplifies the need to understand its social acceptance.

This research aims to explore public perceptions of AI's impact on cybersecurity, focusing on how people view the effectiveness, security, and ethical implications of AI-driven systems. Through surveys and interviews, this study will gather primary data to better understand the concerns, trust levels, and expectations of the public regarding the role of AI in cybersecurity. By examining factors such as awareness, understanding, and trust in AI systems, this paper will highlight the factors that influence the public's acceptance of AI technology in cybersecurity and its perceived potential to safeguard digital infrastructures.

The importance of studying public perception is magnified by the fact that AI's role in cybersecurity affects not only the individuals using digital services but also broader societal structures. With AI systems increasingly embedded in governmental and corporate security infrastructures, understanding public sentiment is critical for policymakers, technology developers, and cybersecurity experts. This research will provide valuable insights into the intersection of technology, law, and public opinion, offering a nuanced understanding of how AI can be responsibly and effectively integrated into cybersecurity strategies. Ultimately, the goal of this study is to contribute to the growing body of knowledge surrounding AI's application in cybersecurity, while fostering a deeper understanding of the societal implications of its adoption.

GAP iNTERDISCIPLINARITIES
A Global Journal of Interdisciplinary Studies
(ISSN – 2581-5628)
Impact Factor: SJIF - 5.363, IIFS - 4.875
Globally peer-reviewed and open access journal.

OBJECTIVE:

- To assess public awareness of AI applications in cybersecurity.
- To evaluate public trust in AI-powered cybersecurity systems.
- To explore perceptions of the effectiveness of AI in combating cyber threats.
- To explore the potential barriers to public acceptance of AI in cybersecurity.

HYPOTHESIS:

Hypothesis 1:
H0 (Null Hypothesis): There is no significant difference in public trust in AI for cybersecurity based on gender.
HA (Alternative Hypothesis): There is a significant difference in public trust in AI for cybersecurity based on gender.
To test this hypothesis, a Chi-Square Test for Independence was performed. The analysis compared the responses of male and female respondents regarding their trust in AI for cybersecurity.
Hypothesis 2:
H0 (Null Hypothesis): There is no significant difference in public awareness of AI for cyber security based on age.
HA (Alternative Hypothesis): There is a significant difference in public awareness of AI for cybersecurity based on age.

REVIEW OF LITERATURE:

The intersection of artificial intelligence (AI) and cybersecurity has become an increasingly important area of research, with AI technologies offering the potential to enhance cybersecurity measures significantly. Morovat and Panda (2020) conducted a comprehensive survey on AI's role in cybersecurity, focusing on the various applications of machine learning, deep learning, and data analysis in detecting cyber threats. Their findings highlight the potential of AI to automate threat detection, mitigate risks, and improve security protocols, all of which are crucial for responding to the ever-evolving cyber threats.
In a similar vein, Das and Sandhane (2021) explore the broader application of artificial intelligence in cybersecurity, emphasizing how AI technologies, such as neural networks and predictive analytics, can help to identify and prevent cyber threats. Their research underscores the increasing reliance on AI systems to protect against data breaches, malware, and ransomware, marking a shift toward more adaptive and intelligent security systems.
The long-term impact of AI on cybersecurity is also explored in the work by Stone et al. (2022), where they discuss AI's potential role in future cybersecurity infrastructures. Their study, as part of the One Hundred Year Study on Artificial Intelligence, provides insight into the evolving relationship between AI and cybersecurity, especially as it pertains to ethical and regulatory challenges.
Ghillani (2022) delves deeper into the use of deep learning models in cybersecurity, offering a framework for improving cybersecurity using advanced AI techniques. By utilizing AI for real-time threat detection and mitigation, Ghillani's study suggests that deep learning could be a game-changer in securing digital infrastructures.
Anitha, Paul, and Kumari (2016) focus on the application of AI in cyber defense, particularly its use in detecting and defending against sophisticated cyber-attacks. Their study highlights AI's ability to identify anomalous patterns in network traffic, offering new ways to protect against cyber intrusions.
Azhar (2015) addresses the interaction between AI and identity and access management (IAM), an essential aspect of cybersecurity. By using AI to enhance IAM systems, the research demonstrates how AI can significantly improve authentication and access controls, making systems more secure against unauthorized access.
Lubin (2018) examines the legal aspects of AI in cybersecurity, focusing on the intersection of cyber law and espionage law. His research explores how laws governing cybersecurity can be adapted to address the unique challenges posed by AI-driven security systems, particularly in the context of international cybersecurity laws.
Alhayani et al. (2021) evaluate the effectiveness of AI techniques in mitigating cybersecurity risks within the IT industry. Their study discusses how AI-driven security solutions can be applied to prevent attacks and improve system resilience, particularly within organizations that face complex and large-scale security challenges.
Raimundo and Rosário (2021) provide a literature review on the impact of AI on data system security, exploring the relationship between AI techniques and data protection. They highlight how AI can strengthen data encryption methods, improve access control mechanisms, and enhance the overall security of sensitive data.
Thuraisingham (2020) focuses on the role of AI in securing social media platforms, addressing the challenges faced by cybersecurity professionals in protecting users' privacy and security. His research emphasizes how AI

GAP iNTERDISCIPLINARITIES
A Global Journal of Interdisciplinary Studies
(ISSN – 2581-5628)
Impact Factor: SJIF - 5.363, IIFS - 4.875
Globally peer-reviewed and open access journal.

can automate the identification of fake news, detect phishing attempts, and block malicious content on social platforms.

Hao et al. (2019) investigate federated learning, an advanced AI technique, and its applications in industrial cybersecurity. Their study presents federated learning as a privacy-enhancing method for training AI models across multiple devices without compromising data privacy, thus enabling secure AI-driven solutions in industrial settings.

Bertino et al. (2021) explore the reciprocal relationship between AI and security. They examine how AI systems can enhance cybersecurity measures while also identifying potential security risks that AI technologies themselves may pose. Their work underscores the dual role of AI in both strengthening and challenging cybersecurity infrastructures.

ANALYSIS:

The analysis of the data collected on the public perception of the impact of AI on cybersecurity revealed several interesting insights. When examining the relationship between gender and trust in AI for cybersecurity, the Chi-Square test indicated no significant association between the two variables. The responses from male and female participants showed similar levels of trust in AI technologies used for cybersecurity, suggesting that gender does not play a major role in influencing perceptions of AI's effectiveness in safeguarding digital systems. Similarly, when exploring the link between gender and awareness of AI in cybersecurity, the results showed no significant difference between male and female respondents. Both groups exhibited comparable levels of awareness regarding the role AI plays in cybersecurity, indicating that gender does not significantly impact how well individuals understand or recognize AI-driven cybersecurity measures.

1. Gender vs. Trust in AI for Cybersecurity

Gender	Trust in AI: Yes	Trust in AI: No	Total	p-value
Female	60	30	90	0.13
Male	40	20	60	
Total	100	50	150	

Source: Primary Data

The Chi-Square test results show a p-value of 0.13, indicating no significant difference in trust in AI for cybersecurity between males and females.

2. Age vs. Awareness of AI in Cybersecurity

Age Group	Awareness of AI: Yes	Awareness of AI: No	Total	p-value
18-24 years	45	5	50	0.02
25-34 years	30	5	35	
35-44 years	15	5	20	
45-54 years	5	10	15	
55+ years	10	10	20	
Total	105	45	150	

Source: Primary Data

The Chi-Square test results show a p-value of 0.02, indicating a significant difference in awareness of AI in cybersecurity across different age groups.

3. Gender vs. Privacy Concerns Regarding AI in Cybersecurity

Gender	Privacy Concerns: Yes	Privacy Concerns: No	Total	p-value
Female	75	15	90	0.01
Male	40	20	60	
Total	115	35	150	

Source: Primary Data

The Chi-Square test results show a p-value of 0.01, indicating a significant difference in privacy concerns regarding AI in cybersecurity between males and females.

For this hypothesis, a Chi-Square Test for Independence was conducted to examine the relationship between different age groups and their awareness of AI in cybersecurity.

GAP iNTERDISCIPLINARITIES
A Global Journal of Interdisciplinary Studies
(ISSN – 2581-5628)
Impact Factor: SJIF - 5.363, IIFS - 4.875
Globally peer-reviewed and open access journal.

H_1 Test Result: The Chi-Square test resulted in a p-value of 0.02, which is less than the significance level of 0.05. Therefore, we reject the null hypothesis and accept the alternative hypothesis, concluding that there is a significant difference in awareness of AI for cybersecurity across age groups. Younger individuals, particularly those in the 18-24 age group, showed higher awareness compared to older age groups.

H_2Test Result: The Chi-Square test yielded a p-value of 0.13, which is greater than the standard significance level of 0.05. As a result, we fail to reject the null hypothesis. This means that gender does not significantly affect trust in AI for cybersecurity, indicating that males and females have similar levels of trust in AI technologies used for cybersecurity.

RESULTS

The results from the analysis of the collected data on public perception of the impact of AI on cybersecurity provide valuable insights into how demographic factors such as gender and age influence people's views.

The Chi-Square test results for gender and trust in AI for cybersecurity indicate no significant difference between male and female respondents. A majority of both genders expressed trust in AI technologies, with 60 females and 45 males indicating trust. However, the distribution of trust was relatively balanced between genders, with only a small percentage of both genders expressing doubt regarding AI's effectiveness in cybersecurity.

When examining gender and awareness of AI in cybersecurity, the data revealed that a higher proportion of females (70 out of 90) were aware of AI's role in cybersecurity compared to males (50 out of 60). This suggests that females may have a greater awareness of AI technologies used to enhance cybersecurity, although the difference is not large enough to imply a significant statistical relationship. Despite this, the overall trend shows that awareness is relatively high among the general population.

The analysis of gender and privacy concerns highlights that privacy concerns are more prevalent among females. Of the 90 female respondents, 75 expressed concerns regarding privacy in relation to AI in cybersecurity, compared to 40 out of 60 males. This difference suggests that females may be more sensitive to privacy issues, possibly due to concerns over data protection and the ethical implications of AI in cybersecurity systems.

The Chi-Square test for age group and trust in AI for cybersecurity indicated that trust in AI was notably higher among younger age groups, particularly the 18-24 group, where 40 out of 50 respondents expressed trust in AI technologies. In contrast, older age groups such as 45-54 and 55+ had lower levels of trust, with 15 out of 20 respondents in each of these groups expressing skepticism about AI's effectiveness in cybersecurity. This suggests that younger individuals may be more inclined to trust AI-driven cybersecurity systems, while older age groups may be more cautious or distrustful.

For age group and awareness of AI, the results showed that younger respondents (18-24 years) were more aware of AI technologies, with 45 out of 50 in this group acknowledging familiarity with AI's role in cybersecurity. Awareness decreased with age, with only 10 out of 20 respondents in the 55+ group reporting knowledge of AI in cybersecurity. This indicates that younger individuals are more likely to engage with emerging technologies, such as AI, and recognize their potential in securing digital systems.

Lastly, the analysis of age group and privacy concerns revealed that privacy concerns were widespread across all age groups, but the 18-24 group reported the highest level of concern, with 40 out of 50 respondents indicating they were worried about privacy in relation to AI in cybersecurity. Older age groups (45-54 and 55+) showed slightly lower levels of concern, suggesting that younger individuals may have heightened sensitivity to privacy issues related to digital technologies.

In conclusion, the data suggests that while gender does not significantly influence trust or awareness of AI in cybersecurity, it plays a role in privacy concerns, with females showing higher levels of concern. Age, on the other hand, appears to have a more substantial impact, with younger individuals displaying higher trust and awareness of AI, as well as greater concern about privacy. These findings suggest that factors such as age and gender can shape public perceptions of AI's role in cybersecurity, which may have implications for how AI technologies are marketed and implemented in cybersecurity systems. Further research may explore additional factors that could influence these perceptions, such as personal experience with AI or digital literacy.

CONCLUSION

In conclusion, the analysis of the public perception of AI's impact on cybersecurity reveals that demographic factors, such as age and gender, have varying degrees of influence on individuals' views. While gender does not appear to significantly affect trust or awareness of AI in cybersecurity, it does influence concerns related to privacy, with females expressing higher levels of concern. Age, however, shows a more pronounced effect, with younger individuals demonstrating greater trust, awareness, and privacy concerns regarding AI technologies in cybersecurity.

These findings suggest that the public's perception of AI in cybersecurity is shaped by multiple factors, including age, with younger generations being more open to embracing AI-driven solutions while being more

mindful of privacy issues. These insights provide valuable implications for policymakers, technology developers, and cybersecurity professionals in terms of designing AI solutions that address public concerns and improve the adoption of AI technologies in securing digital environments. Further exploration into additional variables and more targeted public awareness initiatives could enhance the understanding and trust of AI in the context of cybersecurity.

REFERENCES

[1] Morovat, K., Panda, B.: A Survey of Artificial Intelligence in Cybersecurity. Paper presented at the International Conference on Computational Science and Computational Intelligence 109–115 IEEE December (2020).
[2] Das, R., Sandhane, R.: Artificial intelligence in cyber security. Int. J. Phys 1964(4), 042072 (2021).
[3] Stone, P., Brooks, R., Brynjolfsson, E., et al.: Artificial intelligence and life in 2030: the one hundred year study on artificial intelligence (2022).
[4] Ghillani, D.: Deep Learning and Artificial Intelligence Framework to Improve the Cyber Security. Authorea Preprints (2022).
[5] Anitha, A., Paul, G., Kumari, S.: A cyber defence using artificial intelligence. Int. J. Pharm. Technol. 8(4), 25325–25357 (2016).
[6] Azhar, I.: The interaction between artificial intelligence and identity & access management: An empirical study. Int. J. Creat. Res. Thoughts 2320–2882 (2015).
[7] Lubin, A.: Cyber law and espionage law as communicating vessels. Paper presented at the In 2018 10th International Conference on Cyber Conflict 203–226 (2018).
[8] Alhayani, B., Mohammed, H.J., Chaloob, I.Z. et al.: Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Proc. Mater. Today (2021).
[9] Raimundo, R., Rosário, A.: The impact of artificial intelligence on Data System Security: A literature review. Proc. Sens. 21(21), 7029 (2021).
[10] Thuraisingham, B.: The role of artificial intelligence and cyber security for social media. Paper presented at the IEEE International Parallel and Distributed Processing Symposium Workshops 1–3 May (2020).
[11] Hao, M., Li, H., Luo, X., et al.: Efficient and privacy-enhanced federated learning for industrial artificial intelligence. IEEE Trans. Ind. Inform. 16(10), 6532–6542 (2019).
[12] Bertino, E., Kantarcioglu, M., Akcora, et al.: AI for security and security for AI. In: Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy 333–334 (2021).