



Impact of Digital Literacy on Artificial Intelligence Based Cyber Security Adoption Among Generation Z

Dr. Vidya M¹, Dr. Rekha M²

¹Assistant Professor of Commerce (SG), The Tamil Nadu Dr. Ambedkar Law University, Chennai, TamilNadu, India

²Assistant Professor, Dept. of Commerce, SDNB Vaishnav College for Women, Chennai, TamilNadu, India

Emails: drmvidyatndalu@gmail.com¹, rekha.m@sdbnc.edu.in²

Abstract

Artificial intelligence (AI) is growing at a fast pace and has changed the protocols of cyber security by providing proactive security, automated risk analysis, and real time threat identification. Gen Z is one of the most digitally connected demographic groups, and knowing the factors that impact their acceptance of AI based cyber security solutions has become more important. The study explores the effect of digital literacy of Generation Z users on the acceptance of AI based cyber security products. This study used a quantitative research design by administering a structured questionnaire to the members of Generation Z. The research framework investigates the relationship between digital literacy and behavioral intention to adopt AI-based cyber security, taking into account perceived utility, perceived ease of use, trust in AI technologies, and privacy concerns. The proposed relationships were evaluated using statistical techniques such as descriptive analysis, Chi-square and ANOVA. The results are expected to demonstrate that increasing levels of digital literacy significantly improve Generation Z's readiness to use AI-driven cyber security products. The results indicate that strong digital skills are associated with more proactive cyber safety behaviors, higher levels of trust in automated protection, and awareness of the benefits of AI enhanced security systems.

Keywords: Digital Literacy, Generation Z, Cyber Security, Artificial Intelligence (AI), Technology.

1. Introduction

The emergence of digital technologies has changed dramatically the way people communicate, share information and interact. In addition to this, cyber threats, including phishing attacks, malware, identity theft and data breaches have become more sophisticated, making the need for cyber security technologies more urgent. Artificial Intelligence (AI) has been identified as one of the instruments in cyber security that helps detect threats, assess risks and perform predictive analysis in order to improve digital protection (Buczak & Guven, 2016). The application of AI-powered cyber security systems is getting more common in order to protect the digital environment from possible threats and increase its security. Generation Z (Gen Z) is a term used to describe the generation of young people who were born between 1997 and 2012. Gen Z is considered to be the first generation

of full-fledged digital natives as the usage of smartphones, social media, cloud computing and other online technologies by them is high. This makes them vulnerable to various cyber security threats. As a result, the determination of factors that influence the adoption of AI-powered cyber security systems by this generation has become an important field of research. Digital literacy can be viewed as one of such factors. It implies the ability of people to efficiently use digital technologies for accessing, evaluating, creating and communicating information (Ng, 2012). Higher level of digital literacy is related to the higher awareness of online threats, digital responsible behavior and proper usage of technology. Earlier, technology adoption literature showed the importance of such factors as perceived usefulness, perceived ease of use, trust and privacy concerns for the formation of people's



perception of new technology (Davis, 1989). At the same time, there is a lack of research on the impact of digital literacy on the adoption of AI-based cyber security technology by Generation Z. The purpose of the current study is to fill this gap. The findings are expected to be beneficial for the fields of cyber security and technology acceptance.

2. Review Of Literature

According to Ng (2012), digital literacy involves not only skill in the use of digital devices but also cognitive and socio-emotional skills necessary for meaningful engagement with digital media. The research shows that people who possess higher digital literacy can effectively evaluate information on the Internet, recognize various risks related to online activity, and use technologies responsibly. This is particularly important within the scope of cyber security because one's awareness of potential risks and the ability to make sound decisions are crucial aspects of protecting oneself from cyber threats. The research conducted by Buczak and Guven (2016) was focused on the role of machine learning and data mining technologies in cyber security. As a result of the research, it became clear that the application of AI makes it possible to considerably improve the process of detecting cyber threats by processing large amounts of data instantly. Park and Kim (2020) studied the link between digital literacy and cyber security awareness among college students. It turned out that there was a correlation between levels of digital literacy and the level of cyber security practice. Individuals possessing high levels of digital literacy proved to be more aware of risks connected with using digital technologies and more attentive about their online security. In their study Venkatesh et al. (2003) based on Unified Theory of Acceptance and Use of Technology (UTAUT) identified four predictors of technology adoption such as performance expectancy, effort expectancy, social influence and facilitating conditions. This framework allows comprehending the adoption process in general and gives an opportunity to understand how users accept and use innovative

technologies. The researchers claim that individual capabilities and technological awareness affect adoption intentions, which is especially important in the field of AI-enhanced cyber security. Shin (2021) investigated the trust in Artificial Intelligence and came to the conclusion that trust is crucial for forming users' intention to adopt AI technologies. It was found out that users who perceive AI technologies as trustworthy, transparent and effective tend to accept automation decisions made by AI. Trust was revealed as a mediator of relationship between technological competencies and adoption of AI. Another factor that is a barrier to technology adoption is related to the issues of privacy and data protection. According to Smith, Dinev, and Xu (2011) people are usually reluctant to adopt innovative digital technologies because of the risks of their personal data being misused and violated.

2.1. Research gap

Even though previous literature has examined digital literacy, technology acceptance, cyber security awareness, and trust in AI separately, there has not been much work done that examines the effect of the interrelationship between digital literacy and the other three factors on the use of AI-driven cyber security solutions by generation Z. The above observation highlights the need for more research to be done on how digital literacy affects perception and trust in AI-driven cyber security technologies and behavioral intentions to use such technology.

2.2. Research Methodology

The systematic method used to gather data and information for efficient decision making is referred to as research methodology. The nature of the current study is descriptive. 362 respondents from various Gen Z age groups provided answers using a purposive sample technique. To gather the necessary data about cyber security, a well-structured questionnaire was used. The primary data used in the study were examined. Furthermore, secondary data was gathered from websites and journals and combined for reference.

3. Objectives

- To find out demographic profile and Gen Z intention of the respondents[1 – 10].
- To examine the association between demographic profile and accept AI security provides accurate threat detection.
- To determine the difference between AI based Cyber Security adoption and Gen Z.
- To examine the relationships between Digital Literacy, Technology Acceptance, Cyber Security Awareness and Trust in AI.As shown in Table 1 Percentage Analysis.

4. Data Analysis

4.1.Percentage Analysis

Table 1 Percentage Analysis

PROFILE	CATEGORY	PERCENTAGE
Gender	Female	47.5
Age	21 years – 22 years	37.8
Qualification	Bachelor's degree	55.8
Income (Monthly)	Rs. 30000 – Rs. 40000	36.5
Marital status	Married	61

From the table 1 shows that the demographic profile of Gender: 47.5% of the respondents were male while 52.5 were female. Age: 10.5% of the respondents were in the age group of below 20 years; 37.8% belonged to the age group of 21 – 22 years; 33.5% of the respondents were in the age group of 23 – 24; 18.2% of the respondents were in the age group of 25 – 27 years. Educational qualification: 5% of the respondents completed

their SSCL, 22.1% completed their HSC, 55.8% completed bachelor's degree and 17.1% of the respondents completed their master's degree. Monthly income: 13% of the respondents were earning less than Rs. 20, 000; 24.3 % were earning Rs. 20,000 – 30,000 monthly; 36.5% had an income between Rs. 30,000 - 40,000 ; 20.2% were earning Rs. 40,000 – 50,000 and 6% were earning & above Rs.50,000 monthly. Marital status: 39% of the respondent was unmarried, while 61% were married[11 – 18].

4.2.Chi-Square test

Ho There is no significant association between demographic Profile and accept AI security provides accurate threat detection

H1 There is a significant association between demographic Profile and accept AI security provides accurate threat detection.As shown in Table 2 Chi-Square test.

Table 2 Chi-Square test

PROFILE	CHI VALUE	DF	SIG. VALUE
Gender	.011	1	.918
Age	4.017	3	.260
Qualification	1.955	3	.582
Income (Monthly)	2.679	4	.613
Marital status	.096	1	.757

From the above table 2 shows that the demographic profile of Gender, Age, Qualification, Income and Marital status have the significance level of above 0.05. Hence, prove that there is no significant association between Gender, Age, Qualification, Income, Marital status and accept AI security

provides accurate threat detection.

4.3. One way ANOVA

- **H₀** There is no significant difference between AI based Cyber Security adoption and Gen Z Age category.
- **H₁** There is a significant difference between AI based Cyber Security adoption and Gen Z Age category. As shown in Table 2 Chi-Square test.

Table 2 Chi-Square test

PROFILE	CHI VALUE	DF	SIG. VALUE
Gender	.011	1	.918
Age	4.017	3	.260
Qualification	1.955	3	.582
Income (Monthly)	2.679	4	.613
Marital status	.096	1	.757

From the above table 2 shows that the demographic profile of Gender, Age, Qualification, Income and Marital status have the significance level of above 0.05. Hence, prove that there is no significant association between Gender, Age, Qualification, Income, Marital status and accept AI security provides accurate threat detection.

4.4. One way ANOVA

- **H₀** There is no significant difference between AI based Cyber Security adoption and Gen Z Age category.
- **H₁** There is a significant difference

between AI based Cyber Security adoption and Gen Z Age category.

Table 3 One-way ANOVA

ADOPTION	F VALUE	SIG. VALUE
Personal Data Protection	1.383	.248
Mobile Security Usage	.979	.403
Confidence in AI Security	.847	.469
Adequacy of Current Protection	.675	.568
Willingness to Use AI Security	.732	.534
Effectiveness of AI Security Tools	.720	.541
Awareness of AI Security Tools	.395	.757
Influence of Online Reviews	1.677	.172
Future Adoption of AI Security	2.469	.062

From the above table 3 shows that the Personal Data Protection, Mobile Security Usage, Confidence in AI Security, Adequacy of Current Protection, Willingness to Use AI Security, Effectiveness of AI Security Tools, Awareness of AI Security Tools, Influence of Online Reviews, Future Adoption of AI Security have the significance level of above 0.05. Hence, prove that there is no significant difference between AI based Cyber Security adoption and Gen Z Age category.

4.5. Correlation Analysis

- **H₀** There is no significant relationship between Digital Literacy (DL), Technology Acceptance (TA), Cyber Security Awareness (CSA) and Trust in AI (TAI)
- **H₁** There is a significant relationship between Digital Literacy (DL), Technology Acceptance (TA), Cyber Security Awareness (CSA) and Trust in AI (TAI) as

shown in Table 4 Correlation matrix

Table 4 Correlation matrix

	DL	TA	CSA	TAI
DL	1			
TA	-.189**	1		
CSA	.570**	.003	1	
TAI	-.180**	.275**	-.029	1
N	362	362	362	362

Correlation is significant at the 0.01 level (2-tailed). From the above table 4 shows that to examine the relationships between Digital Literacy (DL), Technology Acceptance (TA), Cyber Security Awareness (CSA) and Trust in AI (TAI) among 362 respondents, a Pearson correlation was conducted. The results show a moderate positive and statistically significant correlation between Digital Literacy and Cyber Security Awareness ($r = 0.570$, $p < 0.01$) which means that higher digital skills are related to greater awareness of cyber security practices and threats. On the other hand, Digital Literacy was found to have a weak yet significant negative correlation with both Technology Acceptance ($r = -0.189$, $p < 0.01$) and Trust in AI ($r = -0.180$, $p < 0.01$), suggesting that those with higher digital skills might be more critical and cautious toward emerging technologies and AI-based systems. Furthermore, Technology Acceptance is positively and significantly related to Trust in AI ($r = 0.275$, $p < 0.01$), which means that people with a higher level of openness to technological innovation tend to have a greater degree of trust in AI-based applications. However, the correlation between Technology Acceptance and Cyber Security Awareness ($r = 0.003$, $p > 0.05$) and between Cyber Security Awareness and Trust in AI ($r = -0.029$, $p > 0.05$) were not statistically significant, indicating no significant direct relationships between these constructs. The results underline the significance of digital literacy for improving cyber security awareness, and point to the importance of technology acceptance as a key antecedent of trust in AI, providing useful insights

into the behavioral aspects related to the acceptance of AI-based cyber security.

5. Results And Discussion

5.1.Results

The findings of the study show that digital literacy is an important factor in Generation Z understands of cyber security. There was a significant positive correlation between digital literacy and cyber security awareness ($r = .570$, $p < .01$), suggesting that the more digitally literate are more aware of cyber security. The negative correlation between digital literacy and technology acceptance and trust in AI indicates a more skeptical evaluation of AI-based technologies. Acceptance of technology is important for building trust in AI-driven security solutions, as shown by the positive correlation between technology acceptance and trust in AI ($r = .275$, $p < .01$). In addition, chi-square and t-test analyses found no significant differences in terms of the adoption-related factors or demographic features ($p > .05$).

5.2.Discussion

The findings emphasize the importance of digital literacy in raising awareness of cyber security and in shaping the Generation Z attitudes towards the adoption of AI-based cyber protection. The results suggest a significant positive correlation between digital literacy and cyber security awareness, meaning that people who are digitally literate are more likely to be aware of cyber threats and adopt safe online practices. Interestingly, there are negative correlations between digital literacy, technology acceptance and trust in AI. This could imply that digitally literate users may be more prone to be cautious and critical when evaluating AI-powered security solutions, consistent with concerns over algorithmic reliability, privacy, and transparency. Moreover, the positive association between technology acceptance and trust in AI highlights that respondents who view technology as beneficial are more likely to develop trust in AI-based security solutions. The lack of significant demographic effects suggests that cognitive and behavioral factors, rather than socio demographic

characteristics, are the primary drivers of AI-based cyber security adoption. These findings are in line with previous studies showing that technology acceptance is still a strong predictor of trust and intention to adopt in new digital contexts and that digital literacy is a facilitator of cyber resilience and informed technology use (Ajzen, 1991; Davis, 1989; Ng, 2012; Venkatesh et al., 2003).

Conclusion

The Conclusion of the study found that digital literacy, a basic determinant of cyber security awareness, has a significant influence on adopting AI-based cyber security solutions by Generation Z. The findings show that digitally literate people are better able to make decisions about AI-enabled security technology, because they have a better understanding of cyber security practices and risks. Demographic factors did not significantly influence adoption behavior, indicating that the primary drivers for AI-based cyber security adoption are knowledge, awareness and views on technology, although technology acceptance has a positive contribution to trust in AI. Therefore, educational programs and legislative changes that improve digital literacy and awareness of AI security will improve cyber resilience and encourage younger generations to responsibly use AI-driven cyber security solutions.

References

- [1].Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211.
- [2].Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE access*, 8, 137293-137311.
- [3].Bhargava, A., Bester, M., & Bolton, L. (2021). Employees' perceptions of the implementation of robotics, artificial intelligence, and automation (RAIA) on job satisfaction, job security, and employability. *Journal of Technology in Behavioral Science*, 6(1), 106-113.
- [4].Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176.
- [5].Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340.
- [6].Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. *arXiv preprint arXiv:1502.03552*.
- [7].Giwah, A. D., Wang, L., Levy, Y., & Hur, I. (2020). Empirical assessment of mobile device users' information security behavior towards data breach: Leveraging protection motivation theory. *Journal of Intellectual Capital*, 21(2), 215-233.
- [8].Gursoy, D., Chi, O. H., Lu, L., & Nunkoo, R. (2019). Consumers acceptance of artificially intelligent (AI) device use in service delivery. *International journal of information management*, 49, 157-169.
- [9].Liang, H., & Xue, Y. L. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the association for information systems*, 11(7), 11–24.
- [10].Ng, W. (2012). Can we teach digital natives digital literacy? *Computers & Education*, 59(3), 1065–1078.
- [11].Park, S., & Kim, Y. (2020). Digital literacy and cyber security awareness among university students. *Journal of Information Security Research*, 12(4), 45–58.
- [12].Prensky, M. (2001). Digital natives, digital immigrants. *On the Horizon*, 9(5), 1–6.
- [13].Ramírez, J. M. (2017). Some criminal aspects of cybersecurity. In *Cyberspace: risks and benefits for society, security and development* (pp. 141-151). Cham: Springer International Publishing.



- [14]. Shin, D. (2021). The effects of explainability and causability on perception, trust, and acceptance of artificial intelligence. *International Journal of Human-Computer Studies*, 146, 102551.
- [15]. Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989–1015.
- [16]. Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy (IJISP)*, 9(1), 26-46.
- [17]. Taddeo, M. (2019). Three ethical challenges of applications of artificial intelligence in cybersecurity. *Minds and machines*, 29(2), 187-191.
- [18]. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425–478.