OPEN ACCESS

Saudi Journal of Engineering and Technology

Abbreviated Key Title: Saudi J Eng Technol
ISSN 2415-6272 (Print) |ISSN 2415-6264 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Original Research Article

AI-Powered Scams and Deepfakes in Tertiary Institutions in Enugu State, Nigeria: The Roles of Cybersecurity Awareness, Digital Literacy, and Media Literacy in Students' Fraud Detection Preparedness

Adesegun Nurudeen Osijirin[1]*, Shamsudeen Mohammed Sada[1], Victor Utibe Edmond[2], Leonard C. Anigbo[3], Oliver Okechukwu[3]

[1]Department of Healthcare Management, Federal University of Allied Health Sciences, Enugu, Nigeria
[2] Department of Health Information Management, Federal University of Allied Health Sciences, Enugu, Nigeria
[3]Department of Mathematics and Computer Science Education, Enugu State University of Science and Technology, Enugu State, Nigeria

DOI: https://doi.org/10.36348/sjet.2026.v11i04.021 | **Received:** 19.02.2026 | **Accepted:** 13.04.2026 | **Published:** 28.04.2026

***Corresponding author:** Adesegun Nurudeen Osijirin
Department of Healthcare Management, Federal University of Allied Health Sciences, Enugu, Nigeria

Abstract

The rapid advancement of artificial intelligence (AI) technologies has significantly transformed digital communication while simultaneously enabling sophisticated cyber threats, particularly AI-powered scams and deepfake-based deception. Deepfake technologies, which involve the generation of highly realistic synthetic audio-visual content, are increasingly exploited for impersonation, fraud, and misinformation, thereby posing serious risks to digital trust and cybersecurity. In Nigeria, the widespread adoption of digital platforms among tertiary institution students has heightened their exposure to such threats. This study examined the roles of cybersecurity awareness, digital literacy, and media literacy in shaping students' preparedness to detect AI-powered scams and deepfakes in tertiary institutions in Enugu State, Nigeria. A descriptive survey design was adopted, involving 469 students selected through a multistage sampling technique from universities, polytechnics, and colleges of education. Data were collected using a structured Google Forms questionnaire and analysed using mean, standard deviation, and independent samples t-test at a 0.05 level of significance. The findings revealed that students possessed cybersecurity awareness, digital literacy, and media literacy to a great extent (Grand Mean = 3.34), and demonstrated preparedness against AI-powered scams and deepfakes to a great extent (Grand Mean = 3.21). However, their ability to detect manipulated media remained relatively weak. No significant difference was found between male and female students in both awareness and preparedness. The study concludes that while students demonstrate reasonable awareness, targeted educational interventions are required to improve their ability to detect sophisticated AI-driven threats. It recommends the integration of deepfake awareness and AI fraud detection strategies into tertiary institution curricula.

Keywords: Artificial Intelligence, AI-Powered Scams, Deepfakes, Cybersecurity Awareness, Digital Literacy, Media Literacy, Fraud Detection Preparedness, Tertiary Institutions, Nigeria.

1. INTRODUCTION

Artificial intelligence (AI) has increasingly become a defining feature of contemporary digital systems, reshaping communication patterns, information dissemination, and user interaction across multiple sectors. While AI-driven innovations have enhanced efficiency and accessibility, they have also introduced complex cybersecurity challenges, particularly through the emergence of AI-powered scams and deepfake-enabled deception. These developments have altered the nature of cyber threats, making them more sophisticated, personalised, and difficult to detect (Kietzmann *et al*., 2020).

Deepfake technology, which enables the creation of highly realistic synthetic audio and video content, represents one of the most significant manifestations of AI-driven risk. Deepfakes are manipulated audio-visual contents capable of deceiving even informed users, thereby contributing to misinformation and erosion of trust in digital systems (Gilbert & Gilbert, 2024). By leveraging advanced machine learning techniques, particularly generative models, deepfakes can convincingly replicate human identities, voices, and behaviours. Although such technologies have legitimate applications, their misuse for impersonation, misinformation, and fraud has raised serious concerns regarding digital trust and information integrity (Westerlund, 2019). The increasing accessibility of deepfake tools further amplifies this risk, as individuals with minimal technical expertise can now generate deceptive content. Deepfake technologies further amplify these risks by enabling impersonation, identity fraud, and misinformation within Nigeria's evolving digital ecosystem (Okeke, 2023).

In a similar vein, AI-powered scams have evolved beyond traditional cyber fraud mechanisms. AI technologies now facilitate advanced attack vectors such as automated phishing, deepfake impersonation, and malware deployment, particularly within Nigeria's rapidly expanding digital economy (Bade *et al*., 2026). Contemporary cybercriminals now deploy intelligent systems capable of analysing user behaviour, tailoring fraudulent messages, and simulating human interaction in real time. These scams often incorporate elements such as phishing, synthetic identities, and voice cloning, thereby increasing their effectiveness and reducing the likelihood of detection (Chen *et al*., 2021). AI-enabled fraud now includes voice cloning, deepfake impersonation, and highly personalised phishing messages, increasing the success rate of cybercriminal activities (Adegoke & Adegoke, 2026). As a result, users are confronted with a rapidly changing threat landscape in which conventional security awareness may no longer be sufficient.

The Nigerian digital environment reflects these global trends. Artificial intelligence has been identified as a critical tool for enhancing cybersecurity through real-time threat detection and predictive analytics, although challenges such as limited expertise and awareness continue to hinder its effectiveness in Nigeria (Eke *et al*., 2025). The expansion of internet access, mobile technologies, and digital financial services has significantly increased online participation among citizens, particularly young people. However, this expansion has also created opportunities for cybercriminal activities. Emerging evidence indicates that AI-enabled fraudulent schemes are beginning to affect digital trust and financial behaviour within Nigeria (Adegoke & Adegoke, 2026). Additionally, the growing concern surrounding deepfake technologies has prompted discussions on cybersecurity regulation and digital safety, especially in relation to cyberfakes and cyberviolence (Ajayi & Adedoyin, 2024).

Within this context, tertiary institution students represent a highly relevant population. Their extensive engagement with digital platforms for academic, social, and financial purposes places them at increased risk of exposure to AI-driven cyber threats. In Enugu State, Nigeria, tertiary institutions including universities, polytechnics, and colleges of education serve as centres of intensive digital interaction. Students routinely utilise online platforms such as learning management systems, social media networks, and electronic payment systems, thereby increasing their vulnerability to sophisticated cyber-attacks.

Addressing these challenges requires more than basic technological competence. It necessitates a combination of cybersecurity awareness, digital literacy, and media literacy, which collectively contribute to an individual's ability to navigate digital environments safely and critically. Cybersecurity awareness equips individuals with knowledge of potential threats and protective behaviours (Kruger & Kearney, 2006), while digital literacy enables effective engagement with digital tools and platforms (Ng, 2012). Media literacy, on the other hand, enhances the capacity to critically evaluate information, identify manipulation, and question the authenticity of digital content (Livingstone, 2004). Empirical evidence shows that students with higher media literacy are significantly better at detecting online fraud and resisting manipulation (Olubori & Adisa, 2025).

Despite the recognised importance of these competencies, existing studies suggest that there remains a disconnect between awareness and practical capability. Studies have shown that although students are aware of cyber threats, many lack practical cybersecurity skills and familiarity with basic protective tools (Aliyu *et al*., 2021). For instance, Okeke (2023) observed that students demonstrate basic cybersecurity awareness but often lack the advanced skills required to address emerging threats. Similarly, Gilbert and Gilbert (2024) found that students' digital practices do not consistently translate into effective protective behaviours, particularly in rapidly evolving cyber environments. This gap becomes more pronounced in the context of AI-powered scams and deepfakes, where detection requires higher-order cognitive and analytical skills.

Media literacy has been identified as a critical factor in mitigating digital deception. Ogunlade *et al*., (2023) established that students with stronger media literacy skills are better able to identify fraudulent content and resist manipulation. However, most existing research examines cybersecurity awareness, digital literacy, and media literacy as independent constructs, without adequately exploring their combined influence on individuals' preparedness to detect AI-driven threats.

Furthermore, there is limited empirical evidence focusing specifically on AI-powered scams and deepfakes within tertiary institutions in Enugu State, despite the increasing relevance of these threats. This gap highlights the need for a more integrated approach that considers multiple dimensions of digital competence within a specific socio-educational context.

Understanding how individuals respond to such threats can be explained through behavioural frameworks that emphasise risk perception and coping mechanisms. Individuals are more likely to adopt protective behaviours when they perceive a threat as severe and believe they possess the capability to mitigate it. In this regard, cybersecurity awareness, digital literacy, and media literacy function as key enabling factors that enhance individuals' capacity to recognise and respond to technological risks.

In addition, the role of gender in shaping digital competencies remains an area of interest. While earlier studies suggested disparities in digital skills between male and female users, increasing access to digital technologies has contributed to a more balanced landscape. However, empirical evidence is still required to determine whether such differences persist in the context of AI-driven cyber threats.

Against this background, this study examines the roles of cybersecurity awareness, digital literacy, and media literacy in influencing students' preparedness to detect AI-powered scams and deepfakes in tertiary institutions in Enugu State, Nigeria.

Research Questions

i. To what extent do students possess cybersecurity awareness, digital literacy, and media literacy required for detecting AI-powered scams and deepfakes?
ii. To what extent are students prepared to detect and respond to AI-powered scams and deepfakes?

Research Hypotheses

The following null hypotheses were tested at 0.05 significance level

i. There is no significant difference between male and female students in their mean ratings of cybersecurity awareness, digital literacy, and media literacy.
ii. There is no significant difference between male and female students in their preparedness to detect AI-powered scams and deepfakes.

2. METHODS

This study adopted a descriptive survey research design to examine the roles of cybersecurity awareness, digital literacy, and media literacy in students' preparedness to detect AI-powered scams and deepfakes in tertiary institutions in Enugu State, Nigeria. The choice of this design was informed by its suitability for collecting quantitative data from a large population and for describing existing conditions without manipulation of variables. It also enables comparison between groups and supports the application of inferential statistical techniques such as the independent samples t-test.

The study was conducted in Enugu State, Nigeria, a prominent educational hub in the South-East geopolitical zone. The state hosts a range of tertiary institutions, including universities, polytechnics, and colleges of education. These institutions are characterised by high levels of digital engagement, as students regularly utilise online platforms for learning, communication, and financial transactions. This widespread use of digital technologies increases students' exposure to emerging cyber threats, including AI-powered scams and deepfake manipulation.

The population of the study comprised undergraduate students in tertiary institutions across Enugu State. A sample size of 469 students was used for the study, which was considered adequate for statistical analysis and generalisation within the study context. A multistage sampling technique was employed to ensure representativeness. Initially, tertiary institutions were stratified into three categories: universities, polytechnics, and colleges of education. Subsequently, two institutions were selected from each category, resulting in a total of six institutions. Finally, students were selected using simple random sampling within the selected institutions.

Data were collected using a structured electronic questionnaire developed by the researchers and administered through Google Forms. The instrument was designed to capture relevant information across three main sections: demographic characteristics, cybersecurity awareness/digital literacy/media literacy, and fraud detection preparedness. Each item in the questionnaire was framed using the first-person pronoun "I" to enhance clarity and respondent engagement. The instrument consisted of twenty items, divided into two clusters. The first cluster measured cybersecurity awareness, digital literacy, and media literacy, while the second cluster measured students' preparedness to detect AI-powered scams and deepfakes. Responses were obtained using a four-point Likert scale, with the following options: Very Great Extent (4), Great Extent (3), Low Extent (2), and Very Low Extent (1). The absence of a neutral option encouraged respondents to provide definitive responses.

The instrument was subjected to face and content validation by experts in Computer Science Education, Cybersecurity, and Measurement and Evaluation. Their feedback ensured that the items were relevant, clear, and aligned with the objectives of the

study. Necessary modifications were made prior to the final administration of the instrument.

The reliability of the instrument was established using Cronbach's Alpha coefficient to determine internal consistency. The results indicated reliability coefficients of 0.82 for the first cluster and 0.79 for the second cluster, with an overall reliability index of 0.81, confirming that the instrument was highly reliable for data collection.

Data collection was carried out electronically by distributing the Google Form link to students through institutional communication channels and social media platforms. Participation was voluntary, and respondents were informed of the purpose of the study. The use of an electronic data collection method ensured efficiency, accessibility, and accurate recording of responses.

The data collected were analysed using the Statistical Package for the Social Sciences (SPSS). Descriptive statistics, specifically mean and standard deviation, were used to answer the research questions, while the independent samples t-test was employed to test the hypotheses at a 0.05 level of significance. Mean scores were interpreted using the following criteria: 3.50–4.00 (Very Great Extent), 2.50–3.49 (Great Extent), 1.50–2.49 (Low Extent), and 1.00–1.49 (Very Low Extent). For hypothesis testing, the null hypothesis was rejected when the p-value was less than or equal to 0.05 and retained when it was greater than 0.05.

Ethical approval for this study was obtained from the appropriate institutional review committee. The study adhered to established ethical standards, including voluntary participation, informed consent, confidentiality, and anonymity of respondents.

3. RESULTS

This section presents the analysis of data collected from 469 students across universities, polytechnics, and colleges of education in Enugu State, Nigeria. The data are analysed in line with the research questions and hypotheses guiding the study. Descriptive statistics (mean and standard deviation) were used to answer the research questions, while the independent samples t-test was employed to test the hypotheses at a 0.05 level of significance.

Research Question 1

To what extent do students possess cybersecurity awareness, digital literacy, and media literacy required for detecting AI-powered scams and deepfakes?

Table 1: Mean Ratings of Students on Cybersecurity Awareness, Digital Literacy and Media Literacy (N = 469)

S/N	Item	Mean (x̄)	SD	Decision
1	I can identify suspicious links and phishing messages	3.41	0.71	GE
2	I am aware that AI can generate deceptive content	3.52	0.66	VGE
3	I can distinguish manipulated audio-visual content	3.08	0.81	GE
4	I verify information before sharing it online	3.27	0.75	GE
5	I am aware of deepfake impersonation risks	3.49	0.70	GE
6	I can recognise patterns of online scams	3.38	0.72	GE
7	I can evaluate the credibility of online sources	3.22	0.74	GE
8	I am aware of AI-generated voice and video deception	3.54	0.65	VGE
9	I use digital skills to protect my personal data	3.31	0.73	GE
10	I can critically analyse digital media content	3.18	0.78	GE

The results in Table 1 indicate that students in tertiary institutions in Enugu State possess cybersecurity awareness, digital literacy, and media literacy required for detecting AI-powered scams and deepfakes to a great extent, with a grand mean score of 3.34.

Items relating to awareness of AI-generated scams (Mean = 3.52) and awareness of AI-driven voice/video deception (Mean = 3.54) recorded the highest mean scores, indicating that students are generally aware of the existence of such threats. However, relatively lower mean scores were observed in items relating to the ability to distinguish manipulated audio-visual content (Mean = 3.08), suggesting that while awareness exists, practical detection skills remain limited.

3.2 Research Question 2

To what extent are students prepared to detect and respond to AI-powered scams and deepfakes?

Table 2: Mean Ratings of Students on Fraud Detection Preparedness (N = 469)

S/N	Item	Mean (x̄)	SD	Decision
1	I can recognise deceptive online messages	3.29	0.73	GE
2	I can verify suspicious audio, video or images	3.44	0.67	GE
3	I protect my personal information online	3.37	0.71	GE
4	I know how to respond to deepfake threats	3.05	0.82	GE
5	I report suspicious digital content when necessary	3.11	0.79	GE

S/N	Item	Mean (x̄)	SD	Decision
6	I use security measures such as strong passwords and 2FA	3.32	0.74	GE
7	I question the authenticity of online information	3.24	0.77	GE
8	I can detect manipulated video or audio content	2.98	0.84	GE
9	I can educate others about cyber threats	3.15	0.78	GE
10	I am confident in handling AI-driven scams	3.12	0.80	GE

Table 2 shows that students are prepared to detect and respond to AI-powered scams and deepfakes to a great extent, with a grand mean score of 3.21.

The highest mean score was recorded for the ability to verify suspicious media content (Mean = 3.44), indicating that students are cautious when interacting with unfamiliar digital content. However, the lowest mean score was observed for the ability to detect manipulated video/audio content (Mean = 2.98), highlighting a significant gap in deepfake detection capability.

3.3 Test of Hypotheses

Hypothesis 1

H_{01}: There is no significant difference between male and female students in their mean ratings of cybersecurity awareness, digital literacy, and media literacy.

Table 3: Independent Samples t-test on Awareness Variables

Gender	N	Mean	SD	df	t-value	p-value	Decision
Male	231	3.31	0.42	467	1.42	0.156	Not Significant
Female	238	3.36	0.39				

Since the calculated p-value (0.156) is greater than the significance level of 0.05, the null hypothesis is not rejected.

This indicates that there is no statistically significant difference between male and female students in their levels of cybersecurity awareness, digital literacy, and media literacy. Both groups demonstrate similar levels of awareness and digital competence.

Hypothesis 2

H_{02}: There is no significant difference between male and female students in their preparedness to detect AI-powered scams and deepfakes.

Table 4: Independent Samples t-test (Preparedness)

Gender	N	Mean	SD	df	t-value	p-value	Decision
Male	231	3.18	0.45	467	1.67	0.096	Not Significant
Female	238	3.25	0.43				

Since the p-value (0.096) is greater than 0.05, the null hypothesis is not rejected.

This implies that there is no significant difference between male and female students in their preparedness to detect AI-powered scams and deepfakes. The results suggest that gender does not significantly influence students' ability to respond to AI-driven cyber threats.

3.4 SUMMARY OF FINDINGS

The major findings of the study are summarised as follows:

i. Students possess cybersecurity awareness, digital literacy, and media literacy to a great extent.
ii. Students are prepared to detect AI-powered scams and deepfakes to a great extent, though practical detection skills remain limited.
iii. There is no significant difference between male and female students in cybersecurity awareness and digital literacy.
iv. There is no significant difference between male and female students in fraud detection preparedness.

4. DISCUSSION

This study investigated the roles of cybersecurity awareness, digital literacy, and media literacy in students' preparedness to detect AI-powered scams and deepfakes in tertiary institutions in Enugu State, Nigeria. The findings provide both theoretical and practical insights into the emerging challenges posed by artificial intelligence-driven cyber threats within an educational context.

The results revealed that students possess cybersecurity awareness, digital literacy, and media literacy to a great extent, indicating a reasonable level of familiarity with digital technologies and online risks. This finding aligns with previous Nigerian studies which suggest that tertiary institution students generally demonstrate moderate to high levels of cybersecurity awareness due to increased exposure to digital platforms

(Okeke, 2023; Gilbert & Gilbert, 2024). This supports earlier findings that cybersecurity awareness does not always translate into effective protective behaviour (Aliyu *et al*., 2021). However, this awareness appears to be largely foundational rather than advanced.

A key finding of this study is the gap between awareness and practical detection ability, particularly in relation to deepfake technologies. While students are aware of AI-generated scams and deception, their ability to distinguish manipulated audio-visual content remains relatively weak. This limitation reflects the growing sophistication of deepfake technologies and the challenges faced by existing detection systems (Gilbert & Gilbert, 2024). This supports the argument that deepfake technologies have evolved beyond the detection capabilities of ordinary users due to their increasing realism and sophistication (Kietzmann *et al*., 2020). Similarly, Westerlund (2019) noted that the rapid advancement of deepfake tools has created new vulnerabilities in digital environments.

The findings also revealed that students are prepared to detect and respond to AI-powered scams and deepfakes to a great extent, although their preparedness is more effective for traditional cyber threats than for AI-driven deception. This suggests that existing cybersecurity knowledge frameworks are still largely oriented towards conventional threats such as phishing and password attacks, rather than advanced AI-enabled fraud. This observation is consistent with Chen *et al*., (2021), who emphasised that artificial intelligence has significantly enhanced the complexity of cyber fraud, thereby requiring more advanced detection skills and adaptive user awareness.

Media literacy emerged as a critical factor in enhancing students' ability to evaluate digital content and detect deception. Students demonstrated relatively strong abilities in questioning the authenticity of online information and verifying suspicious content. This finding is in line with Ogunlade *et al*., (2023), who established that media literacy significantly influences online fraud awareness among university students. It also supports the broader argument that critical thinking and analytical skills are essential for navigating digital environments characterised by misinformation and manipulation (Livingstone, 2004). This reinforces the importance of media literacy as a key determinant of fraud detection capability among students (Olubori & Adisa, 2025).

Digital literacy was also found to contribute to students' preparedness, particularly in terms of navigating online platforms and utilising security features. However, the study highlights that digital literacy alone is insufficient for addressing the complexities of AI-driven threats. This reinforces the need for an integrated approach that combines technical skills with critical media evaluation and cybersecurity awareness.

Another important finding of this study is that there is no significant difference between male and female students in both cybersecurity awareness and fraud detection preparedness. This suggests that gender does not significantly influence digital competence within the study population. This finding reflects the increasing accessibility of digital technologies and the widespread adoption of smartphones and internet services among students, which has reduced traditional gender disparities in digital skills. AI-driven cybersecurity systems require adequate user awareness and institutional support to be effective in mitigating emerging threats.

The implication of this finding is that cybersecurity interventions do not necessarily need to be gender-specific but should instead focus on enhancing the competencies of all students. However, further research may still be required to explore gender differences in other contexts or populations.

The findings of this study underscore the need to move beyond basic cybersecurity awareness towards more advanced and practical training that addresses emerging threats such as AI-powered scams and deepfakes. The study contributes to existing literature by providing empirical evidence from a Nigerian context and by integrating multiple dimensions of digital competence into a unified framework.

5. CONCLUSION

This study examined the influence of cybersecurity awareness, digital literacy, and media literacy on students' preparedness to detect AI-powered scams and deepfakes in tertiary institutions in Enugu State, Nigeria.

The findings revealed that students possess a foundational level of awareness and digital competence, demonstrating cybersecurity awareness, digital literacy, and media literacy to a great extent. However, despite this awareness, their ability to detect sophisticated AI-driven threats, particularly deepfake audio and video manipulation, remains limited. This highlights a critical gap between knowledge and practical application.

The study further established that students are generally prepared to respond to AI-powered scams and deepfakes, although their preparedness is more effective for traditional cyber threats than for emerging AI-based deception. Additionally, the findings indicated that gender does not significantly influence students' awareness or preparedness, suggesting a relatively uniform level of digital competence among male and female students.

In conclusion, the study emphasises that addressing AI-powered cyber threats requires a holistic approach that integrates cybersecurity awareness, digital literacy, and media literacy. Educational institutions must prioritise the development of advanced digital competencies that enable students to critically evaluate digital content and effectively respond to emerging threats.

6. LIMITATIONS OF THE STUDY

This study is not without limitations. The reliance on self-reported data may introduce response bias, as participants may overestimate their abilities. Furthermore, the study was limited to tertiary institutions in Enugu State, which may affect the applicability of the findings. Lastly, the cross-sectional design does not allow for causal inferences. Future studies should consider longitudinal designs and incorporate experimental approaches to assess actual detection capabilities.

7. RECOMMENDATIONS

The following recommendations are proposed based on the findings of this study:

i. Tertiary institutions should integrate AI fraud detection and deepfake awareness into their curricula.
ii. Media literacy programmes should be strengthened to enhance students' critical evaluation skills.
iii. Practical training and simulations should be introduced to improve real-world detection capabilities.
iv. Government and educational stakeholders should develop policies promoting digital safety education.
v. Further research should explore advanced detection tools and behavioural responses to AI-driven threats.

8. ACKNOWLEDGEMENTS

Adesegun Nurudeen Osijirin – Conceptualization, Methodology, Writing (original draft), Formal analysis
Victor Utibe Edmond – Data curation, Resources
Leonard C. Anigbo – Supervision Oliver Okechukwu – Supervision
Shamsudeen Mohammed Sada – Data Curation, Resources

9. Conflict of Interest: The authors declare that there is no conflict of interest.

REFERENCES

- Adegoke, K. R., & Adegoke, T. B. (2026). AI-enabled fraudulent schemes and their effects on consumer trust and digital financial adoption in Nigeria. *SSR Journal of Multidisciplinary*, 3(1), 20–36. https://doi.org/10.5281/zenodo.18228379
- Ajayi, O. & Adedoyin, A. (2024). Implications of deepfakes for cybersecurity in Nigeria.
- Aliyu, A., Aliyu, M., Ahmad, A., & Abdullahi, S. (2021). Investigating cybersecurity awareness among tertiary institutions students in Nigeria. *International Journal of Advances in Engineering and Management*, 3(10), 111–118. https://doi.org/10.35629/5252-0310111118
- Bade, A. M., Babate, A. I., & Bara, M. W. (2026). AI-driven cyber threats and defences in Nigeria's digital economy: A literature review. *International Journal of Research and Innovation in Applied Science*, 11(2), 1505–1511. https://doi.org/10.51584/IJRIAS.2026.110200140
- Chen, H., Chiang, R.H.L. & Storey, V.C. (2021). Artificial intelligence in fraud detection. *IEEE Access*, 9, 152123–152138. https://doi.org/10.1109/ACCESS.2021.3126057
- Eke, C., Ikebude, O. D., & Okure, E. G. (2025). Artificial intelligence and cyber-security in Nigeria: Communicative strategies for risk mitigation and opportunities in digital security. Top Academic Journal of Humanities and Social Sciences, 10(2), 1–16. https://doi.org/10.5281/zenodo.15183395
- Gilbert, C., & Gilbert, M. A. (2024). The role of artificial intelligence (AI) in combatting deepfakes and digital misinformation. *International Research Journal of Advanced Engineering and Science*, 9(4), 170–181.
- Kietzmann, J., Lee, L.W., McCarthy, I.P. & Kietzmann, T.C. (2020). Deepfakes: Trick or treat? *Business Horizons*, 63(2), 135–146. https://doi.org/10.1016/j.bushor.2019.11.006
- Kruger, H.A. & Kearney, W.D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008
- Livingstone, S. (2004). Media literacy and the challenge of new information technologies. *The Communication Review*, 7(1), 3–14. https://doi.org/10.1080/10714420490280152
- Ng, W. (2012). Digital literacy and educational outcomes. *Computers & Education*, 59(3), 1065–1078. https://doi.org/10.1016/j.compedu.2012.04.016
- Ogunlade, O., et al. (2023). Media literacy and online fraud awareness among students.
- Okeke, B. O. (2023). Deepfake technology as an emerging cybersecurity threat: Implications for Nigeria's national security and digital ecosystem. *International Journal of Scientific Research in Science and Technology*, 10(3), 1316–1322. https://doi.org/10.32628/IJSRST23113272
- Olubori, O. O., & Adisa, R. M. (2025). Media literacy competencies and online fraud awareness: A study of social media users at Kwara State

University. *International Journal of Intellectual Discourse*, 8(4), 97–112.

- Westerlund, M. (2019). The emergence of deepfake technology. *Technology Innovation Management Review*, 9(11), 40–53. https://doi.org/10.22215/timreview/1282