UTILIZATION OF AI-DRIVEN THREAT DETECTION TOOLS FOR CYBER-SECURITY IN BUSINESS EDUCATION PROGRAMMES IN UNIVERSITIES IN SOUTH-EAST NIGERIAN: OPPORTUNITIES AND CHALLENGES

Dr. Felicia O. Nwokike
Department of Business and Entrepreneurship Education
Enugu state University of Science and Technology (ESUT), Enugu
Email: ogonnianwokike@yahoo.com

Chizoba Priscillia Onochie-Ogene
Department of Business Education
Federal College of Education
Eha-Amufue
Email: priscszoba@gmail.com,

Abstract

The study aimed to assess the opportunities and challenges of using AI-driven threat detection tools for cybersecurity in Business Education Programmes at universities in South-East Nigeria. A descriptive survey research design was adopted. The population consisted of 82 Business Educators from seven public universities in South-East Nigeria. Due to the manageable population size, the entire population was studied, and no sampling was conducted. Data were collected using a structured 20-item questionnaire, with 74 responses received out of 82. The instrument was validated by three research experts, and their feedback was incorporated to enhance its validity. Two research questions and two null hypotheses were formulated and tested at a significance level of 0.05. The Cronbach's alpha reliability method was used, yielding an overall reliability coefficient of 0.82. Data were analyzed using mean and standard deviation to answer the research questions, while t-test statistics were employed to test the hypotheses. The findings indicate that AI-driven threat detection tools offer opportunities such as protecting intellectual property, enhancing institutional reputation, safeguarding data, encouraging wider adoption, benefiting from real-time monitoring, preparing students for future digital workplaces, and detecting and preventing cyber threats. The study also identified challenges including inadequate ICT infrastructure, limited technical expertise, resistance to technological change, and poor structural facilities in universities. The researchers recommended, among other things, that advocacy for AI-driven threat detection tools is essential in business education programmes to safeguard intellectual property and enhance the reputation of higher education institutions. Additionally, awareness programmes should be implemented to overcome resistance to technological change and promote acceptance of AI-driven cybersecurity systems among educators and stakeholders.

Keywords: Cyber-Security, Business Education, AI-Driven Threat Detection, Opportunities and Challenges

Introduction

Business education is a form of education that equips individuals with practical business knowledge, skills, and competencies required to become productive employees, successful entrepreneurs, and effective managers who can contribute to economic and societal development. Naeem (2019) defined business education as a type of education provided to develop business acumen, capability, and skills in a person which may help him or her to work efficiently and effectively in the future. Similarly, Lokhtina and Kkese (2022) described business

education as education that embraces the teaching and learning of skills and knowledge that can be applied in the business industry. At the university level, Business Education programmes increasingly operate within digitally transformed teaching, learning, research, and administrative environments.

The adoption of digital technologies has transformed how universities teach, how students learn, and how research and administration are managed. The use of technologies such as learning management systems, virtual classrooms, cloud storage, online assessments, digital libraries, and artificial intelligence has improved teaching, learning, research, and administration, making education more efficient, accessible, and interactive. However, this digital transformation has also increased the exposure of universities to cyber-security threats. Large amounts of sensitive information, including students' personal records, examination results, financial data, and research findings, are stored and transmitted electronically, making them vulnerable to attacks by cybercriminals. Deuri (2025) observed that as the digital world expands, cyber-security threats have become a growing concern, particularly in higher education institutions where students actively engage in online activities.

The increasing dependence of universities on digital systems has created a complex cyber-security environment in which institutional networks, databases, learning platforms, and cloud-based services may be exposed to unauthorized access, data breaches, malware, phishing attacks, ransomware, and other forms of cyber threats. These threats can disrupt teaching and learning activities, compromise sensitive institutional information, damage intellectual property, and affect the reputation and integrity of universities. Consequently, universities require effective cyber-security measures that can identify and respond to threats before significant damage occurs.

The increasing sophistication of cyberattacks and the limitations of conventional security approaches have created the need for more adaptive and responsive cyber-security solutions. Ajoku, Ogini, and Cookey (2025) noted that as the sophistication of cyberattacks increases, the need for more adaptive and responsive security solutions becomes paramount. Traditional security systems rely heavily on predefined rules and signatures, which often fail to recognize unknown threats or adapt to new attack methods. Although such systems may be effective in identifying well-established threats, they may fall short when confronted with novel, evolving, or highly sophisticated attacks, such as zero-day attacks and fileless malware. This limitation has highlighted the need for more dynamic and intelligent systems capable of responding to a rapidly changing cyber-security landscape.

One emerging solution is AI-driven threat detection. AI-driven threat detection is the use of artificial intelligence to automatically identify, analyze, and alert computer operators about possible dangers or attacks within their systems. According to Ajoku et al. (2025), threat detection refers to the identification of potential security breaches or malicious activities before they can cause harm to systems or data. AI-driven systems enhance this process by enabling computers to detect suspicious activities that deviate from normal patterns of behaviour, including activities that may be novel or previously unknown.

AI-driven threat detection utilizes technologies such as machine learning and deep learning to analyze large volumes of network traffic, user behaviour logs, and other system interactions in real time. Ajoku et al. (2025) pointed out that AI enhances threat detection by enabling systems to autonomously detect suspicious activities that deviate from baseline behaviour. Similarly, Carpenter (2025) described AI threat detection as the use of artificial intelligence technologies to identify, analyze, and respond to potential security threats in real time.

The utilization of AI-driven threat detection tools provides several opportunities for improving cyber-security in universities. One major capability is real-time monitoring and alerting. AI systems can continuously analyze data from networks, systems, and users to identify anomalies and generate immediate alerts when potential threats are detected. SentinelOne (2026) stated that AI algorithms are capable of continuously analyzing data for anomalies, enabling the early

detection of potential threats before they cause significant damage. Mata (2026) similarly reported that AI identifies threats instantly by analyzing vast data streams across endpoints, networks, and cloud environments.

Another important capability of AI-driven threat detection is its ability to identify emerging and previously unknown threats. Unlike traditional systems that depend largely on known attack signatures, AI systems can learn from patterns of normal and abnormal behaviour and adapt to evolving cyber threats. Ajoku et al. (2025) stated that AI-powered systems can continuously adapt to new threats as they emerge, providing continuous protection without waiting for human intervention. This capability is particularly important in university environments where large numbers of users interact with institutional digital systems on a daily basis.

AI-driven threat detection systems also provide scalability and operational efficiency. As university digital environments expand, large volumes of information can be generated across networks, learning platforms, administrative databases, and cloud services. SentinelOne (2026) stated that AI-based threat detection systems can process large amounts of information without sacrificing performance and can be customized to meet the specific needs of organizations. Mata (2026) added that scalable protection enables organizations to adapt to growing environments and evolving attack surfaces without losing effectiveness.

Another important benefit is the reduction of false positives. Traditional threat detection systems may incorrectly identify normal activities as malicious, resulting in unnecessary alerts and increased workloads for security personnel. AI-enabled systems can reduce false positives by learning patterns of normal behaviour and refining their algorithms over time. Mata (2026) noted that intelligent filtering minimizes alert fatigue and enables security teams to focus on genuine threats. This can improve the efficiency of cyber-security personnel and allow institutions to respond more effectively to actual security incidents.

AI-driven threat detection can further enhance operational efficiency by automating the process of identifying threats, alerting security teams, and supporting timely responses. According to Mata (2026), AI automates threat identification at scale, reducing manual workloads and enabling faster responses. SentinelOne (2026) also stated that AI can automate the process of detecting threats, alerting security teams, and preventing additional threats. These capabilities can be valuable to universities where limited technical personnel may be required to manage increasingly complex digital environments.

Despite the opportunities provided by AI-driven threat detection, its effective utilization may be influenced by several challenges. The deployment and management of AI-driven cyber-security systems may require adequate funding, reliable electricity, modern ICT infrastructure, technical expertise, institutional support, and appropriate policies. In the Nigerian higher education environment, challenges relating to inadequate funding, poor infrastructure, unreliable power supply, limited technical expertise, and resistance to technological change may affect the adoption and effective utilization of emerging technologies. These challenges make it important to examine not only the opportunities provided by AI-driven threat detection tools but also the factors that may hinder their utilization.

From the available literature, there is a knowledge gap between the present study and previous studies. While the present study focuses specifically on the utilization of AI-driven threat detection tools for cyber-security in Business Education programmes in universities in South-East Nigeria, previous studies have focused generally on artificial intelligence in cyber-security and related areas, including studies conducted in other geopolitical zones and sectors. Although some earlier studies have examined cyber-security and artificial intelligence within Nigerian universities and other sectors, little or no empirical research has specifically focused on how Business Education programmes in universities in South-East Nigeria utilize AI-driven threat detection tools to safeguard their digital teaching, learning, research, and administrative environments.

This gap in knowledge makes it necessary to investigate the utilization of AI-driven threat detection tools for effective cyber-security in Business Education programmes in universities in

South-East Nigeria. The study therefore seeks to identify the opportunities available through the utilization of AI-driven threat detection tools and the challenges that may hinder their effective utilization. The findings of the study are expected to provide useful information to Business Educators, university administrators, government, and other stakeholders on how AI-driven threat detection tools can be effectively utilized to strengthen cyber-security and protect digital resources within Business Education programmes.

Statement of the Problem

Universities in South-East Nigeria, like their counterparts worldwide, are increasingly vulnerable to cyber-attacks due to their growing reliance on digital platforms for teaching, research, and administration. These attacks pose serious threats to student records, research outputs, and financial transactions, with consequences that undermine academic integrity, administrative efficiency, and institutional reputation. The situation is further worsened by limited infrastructure, weak policy frameworks, poor awareness, and funding constraints, which collectively heighten institutional exposure to cyber risks. Although advanced technologies such as AI-driven threat detection tools offer real-time monitoring and predictive security, their utilisation in business education programmes within the region remains unknown. If these challenges are not addressed, unchecked cyber-attacks will not only compromise academic performance and administrative operations but also erode the global competitiveness of universities in South-East Nigeria. Hence the need for this study.

Purpose of the Study

The main purpose of this study is to examine how the AI driven threats detection system powered tools can enhance effective cyber-security in business education programmes in universities in South-East Nigeria. Specifically, the study sought to determine the:

1. Opportunities available in utilizing AI-driven threat detection tools for cyber-security in Business Education programmes in universities in South-East Nigeria
2. Challenges hindering the effective utilization of AI-driven threat detection tool in Business Education in universities in South-East Nigeria

Hypotheses

The following null hypotheses will guide the study and will be tested at the 0.05 level of significance:

1. **H_{01}:** The mean rating of Business Educators on the opportunities available in utilizing AI-driven threat detection tools for effective cyber-security in Business Education programmes in universities in South-East Nigeria is not significantly greater than the criterion mean of 2.50.
2. **H_{02}:** The mean rating of Business Educators on the challenges hindering the utilization of AI-driven threat detection tools for effective cyber-security in Business Education programmes in universities in South-East Nigeria is not significantly greater than the criterion mean of 2.50.

Method

The researchers adopted descriptive survey research design since it involved eliciting information from respondents. Descriptive research is a type of research design that involves systematically observing and documenting the characteristics, patterns, and trends of a population or phenomenon without manipulating variables or establishing cause-and-effect relationships (Dovetail Editorial Team, 2023). The descriptive research design, according to Sirisilla (2023), entails observing and gathering information on a particular subject without making an effort to deduce cause-and-effect relationships. Descriptive research aims to describe the relationships, patterns, and trends found in the data as well as to present a complete and accurate picture of the population or phenomenon under study. This design is suitable for the study because the researchers collected data from male and female Business Educators in Universities in South-East Nigeria on opportunities and challenges to the utilisation of AI-Driven threat detection tools.

The population for the study comprised all the 82 Business Educators in the seven public universities in South-East, Nigeria. The population is made up of 51 female and 31 male Business Educators in the public universities in South-East, Nigeria. The entire population was used for the study due to its manageable size. As a result, no sampling was involved in the study. A 20 itemed questionnaire titled "AI-Driven Threat Detection Tools for Cyber-Security Opportunities and Challenges (ADTDSPOC) " developed by the researchers was used for data collection. The instrument had two sections: A and B. Section A contains the respondents bio data while section B was divided into part A and B, with 20 items structured in line with the research questions that guided the study. Part A is on opportunities available in utilizing AI-driven threat detection powered tool for effective cyber-security in business education programmes in universities in South-East Nigeria with 10 items, while part B is on Challenges hindering the effective utilization of AI-driven threat detection tool in business education in universities in South-east Nigeria with 10 items. The response format for the instrument was 4-point scale of Strongly Agree (SA)), Agree (A) , Disagree(D) ,Strongly Disagree (SD) with the following numerical values: 4,3,2, &1 assigned to them.

In order to ensure the validity of the instrument, draft copies of the instrument together with the research title, purpose of the study, research questions, hypotheses, and the developed instrument were given to three experts. Two of the experts where from the Department of Business and Entrepreneurship Education, while one of the experts was from the Department of Mathematics and Computer Education (Measurement and Evaluation Unit). They were requested to assess the relevance, adequacy, suitability and comprehensiveness of the items in addressing the research questions as well as the clarity of the instruction to the respondents. Their comments, suggestions and advice were used in restructuring the instrument. The questionnaire was administered to the respondents by the researchers with the help of two research assistants that were properly briefed on the content of the questionnaire and its administration to ensure that the questionnaire was properly administered. The research assistants assisted in the retrieval of the completed questionnaire Out of 82 administered instruments; only 74 copies of the questionnaire representing 90% were retrieved. The statistical tools for data analyses for the study was mean, standard deviation and t-test statistic. Mean and standard deviation were used in answering the research questions that guided the study, while t-test statistic was used to test the null hypotheses formulated to guide the study at .05 level of significance. For the decision rule, real limits of numbers were applied. as follows; 3.50 – 4.00 = Strongly Agree (SA) , 2.50 – 3.49 = Agree (A) 1.50 – 2.49 = Disagree (D). 0.00 – 1.49 = Strongly Disagree (SD)
In testing the hypotheses, when $P < .05$, the null hypothesis is rejected while on the other hand when $P > .05$, the null hypothesis is upheld

Results
The data collected and analyzed were presented in tables according to the research questions that guided the study and null hypotheses tested at 0.05 level of significance. The data analyzed were based on the 74 copies of questionnaire retuned.
Table 1: Mean Ratings and Standard Deviation of male and female Business Educators on the opportunities available in utilizing AI-driven threat detection tools for effective cyber-security in business education programmes in universities in South-East Nigeria.

S/N	AI-driven threat detection tools for effective cyber-security Opportunities include:	Male N=28		Female=46		Overall =74		Decision
		X_1	SD_1	X_2	SD_2	X_G	SD_G	
1	detect and prevent cyber threats	2.90	0.79	3.04	0.77	2.97	0.78	Agree
2	improves data protection	3.00	0.79	2.60	0.64	2.80	0.71	Agree
3	reducing the workload of IT staff	2.88	0.60	3.08	0.89	3.00	0.75	Agree
4	provides cost-effective solutions	2.80	0.83	2.83	0.79	2.82	0.81	Agree

5	benefit from real-time monitoring	3.16	0.70	2.78	0.80	2.98	0.75	Agree
6	encourage wider adoption	2.95	0.76	2.93	0.69	2.94	0.72	Agree
7	Enhances confidence in online use	2.85	0.81	2.97	0.67	2.91	0.74	Agree
8	protect intellectual property	3.05	0.94	3.17	0.70	3.11	0.79	Agree
9	enhances institutional reputation	3.20	0.83	2.97	0.61	3.08	0.72	Agree
10	prepares students for future digital workplaces	2.95	0.69	3.03	0.56	3.00	0.63	Agree
	Cluster Mean/SD	**2.97**	**0.77**	**2.94**	**0.71**	**2.96**	**0.74**	**Agree**

The results in table 1 shows that Business Educators in South-East Nigerian universities generally agree that AI-driven threat detection tools provides many opportunities for effective cyber-security in Business Education programmes in universities in South-East the mean ranged from 2.91 (enhance confidence in online use) to 3.11(protect intellectual property). The grand mean of 2.96 generally indicate that there are many opportunities available for utilizing AI-Driven threat detection tools for Business Education programmes in universities in South-East. The standard deviation of 0.74 indicates that the respondent's opinions do not differ remarkably to the itemized.

Table 2: Summary of t-test Analysis of mean response scores of male and female business educators on the Opportunities AI-driven threat detection tools present for cyber-security in business education programmes in universities in South-East Nigeria

Variables	N	t	Df	Sig. (2tailed)	Mean Difference	Std. Error Difference	Decision
Male	28	.106	72	.916	.15000	1.41228	NS
Female	46						

NS= Not Significant

The result of the t-test analysis in Table 2 shows that the t-value at the 0.05 level of significance and 72 degrees of freedom for the items is 0.106, with a significance value of 0.916. Since the significance value of 0.916 is greater than the 0.05 level of significance, the null hypothesis is not rejected. This means that there is no significant difference with respect to the items on the mean response scores of male and female Business Educators regarding the available opportunities for utilizing AI-driven threat detection for cybersecurity in Business Education programmes in universities in South-East Nigeria.

Table 3: Mean Responses and Standard Deviation of male and female business educators on Challenges faced in the use AI-driven threat detection powered tools for cyber-security in business education programmes in universities in South-East Nigeria

S/N	challenges of AI-driven threat detection tools present the following include;	Male N=28		Female N 46		Overall N=74		Decision
		X_1	SD_1	X_2	SD_2	X_G	SD_G	
11.	High cost of installation	3.05	0.89	3.13	0.77	3.09	0.83	Agree
12.	Limited technical expertise	3.13	0.74	2.57	0.51	2.85	0.62	Agree
13.	Inadequate ICT infrastructure	3.45	0.76	2.93	0.61	3.19	0.69	Agree
14.	Resistance to technological change	2.50	0.61	3.20	0.71	2.73	0.66	Agree
15.	government funding	2.70	0.69	2.93	0.69	2.81	0.69	Agree
16.	Epileptic power supply	3.20	0.71	3.10	0.66	3.15	0.68	Agree
17.	Lack of awareness	3.05	0.61	3.37	0.67	3.21	0.64	Agree
18.	Poor funding of Business Education	3.09	0.70	3.33	0.66	3.23	0.68	Agree
19.	Un-inclusive of business educators in curriculum planning	3.10	0.58	3.00	0.79	3.05	0.69	Agree
20.	Poor structural facilities in universities	3.30	0.67	3.10	0.57	3.20	0.62	Agree
	Cluster Mean/SD	**3.06**	**0.69**	**3.07**	**0.66**	**3.05**	**0.68**	**Agree**

The result in table 3 research question two shows that the identified items are the challenges to utilization of AI-Driven threat detection tools for cyber-security in Business Education programmes.

The mean scores ranges from 2.81 to 3.23 with standard deviation ranging from 0.62 to 0.83. A cluster mean of 3.05 indicate that the identified 10 items are the challenges to utilization of AI-driven threat detection tools for cyber-security in Business Education programme, The standard deviation of 0.68 is an indication that the respondents are very close in their responses.

Table 4: Summary of t-test Analysis of mean response scores of male and female business educators on the challenges of AI-driven threat detection tools in universities in South-East Nigeria

Variables	N	t	df	Sig. (2tailed)	Mean Difference	Std. Error Difference	Decision
Male	28	.154	72	.878	.18333	1.19134	NS
Female	46						

NS= Not Significant

The data obtained from the t-test analysis in Table 4 shows that the t-value at the 0.05 level of significance and 72 degrees of freedom for the items is 0.154, with a significance value of 0.878. Since the significance value of 0.878 is greater than the 0.05 level of significance, the null hypothesis is not rejected. This means that there is no significant difference with respect to the items on the mean response scores of male and female business educators regarding the challenges of AI-driven threat detection tools in universities in South-East Nigeria.

Discussion of findings

The findings of this study are discussed based on the research questions that guided the study. Table 1 above shows the responses of the Business Educators on available opportunities for utilization of AI-driven threat detection tools for Business Education programme. Specifically, respondents emphasized that these tools protect intellectual property and enhance institutional reputation. This supports the findings of Zhang, Wang, and Li (2023), who highlighted the transformative impact of AI on intellectual property management, cyber-security, and privacy protection through automation, advanced data analysis, and real-time monitoring.

Similarly, Gemmell (2025) emphasized the importance of safeguarding intellectual property by protecting sensitive data and assets from cyber threats. While acknowledging the risks associated with AI, such as theft or reverse engineering, Gemmell argued that AI is valuable for monitoring, tracking, and detecting infringements, enabling early intervention. Chatwood (2025) also noted that organizations with valuable patents are utilizing AI to review new patents and prevent duplication, strengthening intellectual property protection.

Adenubi, Samuel, and Karimu (2024) extended this discussion to the academic realm, highlighting AI's role in revolutionizing intellectual property, cyber-security, and privacy management in research. They cited WIPO (2019) to show that AI-driven tools are being used globally to detect infringements, monitor plagiarism, and ensure compliance with intellectual property laws. These findings underscore the essential role of AI in safeguarding intellectual property and institutional integrity. Mille (2020) also emphasized that combining behavioral tracking with AI-driven anomaly detection enhances early detection and reduces breaches in educational institutions. Samonte, Dorado, Dulay, and Leyva (2024) highlighted the importance of AI-driven fraud detection and behavioral analytics in financial institutions, while Akintola and Yahaya (2024) emphasized the transformation of fraud detection from reactive to proactive with AI. These insights support the view that AI enhances institutional resilience, trust, and reputation in academic and financial sectors.

The comparison of male and female business educators in Table 2 revealed no significant gender difference in perceptions of AI utilization, aligning with Olom and Atah's (2025) findings in Cross River State, which stated that there was no significant difference in the extent of utilization of artificial intelligence in educational content creation and personalized instruction based on gender. This suggests that the adoption of AI in instructional preparation is influenced more by institutional and infrastructural factors than by gender.

The findings from research question two table 3 identified high installation costs, lack of government and program funding, and inadequate ICT infrastructure as major barriers to effective utilization of AI-driven cyber-security systems by business educators. Additionally, unreliable power supply and poor facilities were highlighted as critical infrastructural challenges. While male respondents focused on technical barriers like outdated systems, female respondents pointed to socio-cultural issues such as resistance to change, lack of awareness, and insufficient funding.

These findings are consistent with Ajibola, Dopamu, and Olurin's (2025) observations that organizations face computational costs, vulnerability to adversarial attacks, and integration challenges when deploying AI systems. Dela Luna (2024) also noted the resource-intensive nature of AI deployment, requiring substantial computational resources and skilled personnel.

Dairo, Odekunle, Bolaji, and Sunday (2025) highlighted systemic barriers faced by Nigerian universities, including unreliable electricity, low internet connectivity, outdated ICT infrastructure, and chronic underfunding, which hinder the adoption of AI solutions in higher education. Similarly, Wada, Izibili, Babayemi, Abdulkareem, Macaulay, and Emadoye (2025) emphasized the budget constraints many institutions face, making it challenging to invest in capital-intensive cyber-security systems. They emphasized the importance of training, ethical frameworks, and tailored policies to overcome these obstacles.

The findings of the second research question underscore the transformative potential of AI in cyber-security but also highlight the infrastructural, financial, and socio-cultural barriers that

impede its effective utilization. Successful adoption of AI-driven cyber-security in higher education requires not only technological investment but also government support, policy development, and institutional reforms.

Conclusion

This study investigated the opportunities and challenges of utilizing AI-driven threat detection system-powered tools for effective cybersecurity in South-East Nigeria. From the findings, the respondents concluded that there are some opportunities for the utilization of AI-driven threat detection system-powered tools for an effective Business Education program. Despite the available opportunities, substantial barriers hinder the utilization of AI-driven threat detection system-powered tools in the universities in South-East Nigeria.

Recommendations

Based on the findings, the study offers the following recommendations:

1. University management should advocate for the integration of AI-driven threat detection tools in business education programmes by university management to protect intellectual property and institutional data, thereby enhancing the reputation and integrity of higher education.
2. Arrangements should be made for awareness programmes to address resistance to technological change and foster acceptance of AI-driven cybersecurity systems among educators and stakeholders.

References

Adenubi, A., Samuel, N., & Karimu, A. Y. (2024, September). AI-driven synergistic model for enhancing intellectual property, cybersecurity, and privacy protection in academic research. *Kuwait Journal of Computer Science, 1*(3), Article 003. https://doi.org/10.47514/kjcs/2024.1.3.003

Afolalu, O., & Tsoeu, M. S. (2025). Cybersecurity in Higher Education Institutions: A Systematic Review of Emerging Trends, Challenges and Solutions. Future Internet, 17(12), 575. https://doi.org/10.3390/fi17120575

Ajibola, O. S., Dopamu, O., & Olurin, O. (2025). Challenges and ethical implications of using AI in cybersecurity. *International Journal of Science and Research Archive, 14*(2), 294–304. https://doi.org/10.30574/ijsra.2025.14.2.0276

Ajoku, C. M., Ogini, P. B., & Cookey, I. B. (2025). The role of artificial intelligence in enhancing threat detection and mitigation in cybersecurity. International Journal of Economics, Environmental Development and Society, 6(1), 122-131.

Akintola, A. A., & Yahaya, S. (2024, October). Application of nanomaterials for heavy metal removal from contaminated environments. *International Research Journal of Modern Engineering and Technology Science, 6*(10), 1091..

Berman, S., & Vorontsov, A. (2021). Artificial intelligence in cybersecurity: Threat detection, mitigation, and prevention. Cybersecurity Review, 4(1), 1-9

Chatwood, R. (2025, January 28). *AI and intellectual property rights*. Dentons. https://www.dentons.com/en/insights/articles/2025/january/28/ai-and-intellectual-property-rights

Dairo, T., Odekunle, Q., Bolaji, & Sunday, D. T. (2025, August). *Transforming university education through usage of artificial intelligence (AI) in Nigeria: Panacea for data-driven approach to curb menace of cyber security*. Paper presented at Lasu Research Fair 7.0, Lagos State University.
https://www.researchgate.net/publication/394259472_Transforming_University_Education_through_Usage_of_Artificial_Intelligence_AI_in_Nigeria_Panacea_for_Data-Driven_Approach_to_Curb_Menace_of_Cyber_Security

Dela Luna, C. (2024, September 16). *AI and cyber security: Innovations & challenges*. KPMG. https://kpmg.com/nl/en/home/insights/2024/06/ai-cyber-security-challenge.htm

Deuri, R. (2025). Enhancing cyber awareness: The role of higher education institutions in building a digitally secure generation. International Journal for Multidisciplinary Research, 7(2).

https://doi.org/10.36948/ijfmr.2025.v07i02.39379

Dovetail Editorial Team. (2023, February 5). *What is descriptive research?* Dovetail. https://dovetail.com/research/descriptive-research

Gemmell, K. (2025, August 3). *How to ensure intellectual property security against AI-driven threats*. Stanzione & Associates, PLLC. https://stanzioneiplaw.com/blog

Igbokwe, I. C (2024). Cyber security in the era of digitalization: Implications for educational management. Unizik Journal of Educational Management and Policy, 6(2), 71–77. https://doi.org/10.60787/ujoemp.v6i2.3892

Lokhtina, I., & Kkese, E. T. (2022). Reflecting and adapting to an academic workplace before and after the lockdown in Greek-speaking Cyprus: Opportunities and challenges. In *Global trends, dynamics, and imperatives for strategic development in business education in an age of disruption* (Chapter 7). IGI Global. https://doi.org/10.4018/978-1-7998-7548-2.ch007

Mata, K. (2026, January 20). AI threat detection: Why it's essential for effective incident response. Swimlane. https://swimlane.com/blog/ai-threat-detection/

Mille, J. A. (2020, March 30). *EdTech – 3 ways artificial intelligence can improve campus cybersecurity*. EdTech Magazine. https://edtechmagazine.com/higher/article/2020/03/3-ways-artificial-intelligence-can-improve-campuscybersecurity-perfcon

Naeem, F. (2019). Harnessing the power of differentiation: A case of Indian business schools. In Kalia, S & Nafees, L (Eds.), *New age admissions strategies in business schools* (pp. 134–148). IGI Global. https://doi.org/10.4018/978-1-5225-9073-6.ch009

Olom, P., & Atah, C. A. (2025). Utilization of artificial intelligence on instructional preparation by business educators in Cross River State. *Mediterranean Journal of Social Sciences, 16*(1), 92. https://doi.org/10.36941/mjss-2025-0008

Samonte, M. J., Dorado, P. L., Dulay, J. B., & Leyva, A. M. (2024, September 20). Enhancing threat detection in financial institutions with AI-driven security information and event management integration. In *Proceedings of the 4th International Conference on Computer Systems (ICCS)* (pp. 85–92). IEEE.

SentinelOne. (2026). *Cybersecurity in higher education: Risks, best practices & frameworks*. https://www.sentinelone.com/cybersecurity-101/cybersecurity/cybersecurity-in-higher-educa

Sirisilla, S. (2023, February 9). *Bridging the gap: Overcome these 7 flaws in descriptive research design*. Enago Academy. https://www.enago.com/academy/descriptive-research-design/

Wada, I. U., Izibili, G. O., Babayemi, T., Abdulkareem, A., Macaulay, O. M., & Emadoye, A. (2025). AI-driven cybersecurity in higher education: A systematic review and model evaluation for enhanced threat detection and incident response. *World Journal of Advanced Research and Reviews, 25*(3), 532–547. https://doi.org/10.30574/wjarr.2025.25.3.0989

Wickramage, N. D. (2022). Effect of transparency in different modalities: A case study in business courses. In J. R. Low-Beer (Ed.), *Integrating transparency in learning and teaching (TILT): An effective tool for providing equitable opportunity in higher education* (Chap. 9). IGI Global. https://doi.org/10.4018/978-1-7998-9549-7.ch009

Zhang, Y., Wang, L., & Li, J. (2023). The Role of Artificial Intelligence in Enhancing Research Protection: Intellectual Property, Cybersecurity, and Privacy. Journal of Academic Research and Innovation, 10(2), 145-162