

CYBERSECURITY CHALLENGES IN THE ERA OF GENERATIVE AI

Shivani Gulati

Assistant Professor
M.G.N College of Education, Jalandhar

Sakshi Sharma

Assistant Professor
M.G.N College of Education, Jalandhar

ABSTRACT

The rapid digital transformation of education has significantly changed the way knowledge is delivered, accessed, and evaluated. Among emerging technologies, Generative Artificial Intelligence has become one of the most transformative innovations in modern education. AI-based learning systems allow students to learn at their own pace while receiving real-time feedback and customized content, which can enhance engagement and academic performance. In addition, the integration of AI with technologies such as augmented reality can create immersive learning environments that improve the overall learning experience. Despite these advantages, the rapid adoption of generative AI in education has raised significant cybersecurity and ethical concerns. Educational institutions store large amounts of sensitive data, including student records, academic information, and research data, making them potential targets for cyberattacks. Generative AI can introduce new security risks such as data privacy violations, AI-generated phishing attacks, deepfakes, and identity manipulation. Furthermore, the increasing use of AI-generated content by students raises concerns about academic integrity and the authenticity of academic work. At the same time, AI technologies can also strengthen cybersecurity in education. AI-powered systems can detect unusual network activities, identify phishing attempts, and automate security monitoring. This study reviews the opportunities and cybersecurity challenges associated with generative AI in education and highlights the need for strong policies, data protection measures, and cybersecurity awareness to ensure the responsible use of AI technologies in educational institutions.

Keywords: Generative Artificial intelligence, Cybersecurity, Education Technology, Data privacy, Academic Integrity

INTRODUCTION

The digital transformation of education has accelerated dramatically over the past decade. Advances in information technology, cloud computing, and artificial intelligence have reshaped the way knowledge is delivered, accessed, and evaluated. Generative artificial intelligence (GenAI) has emerged as one of the most transformative innovations in modern education. AI as “the capacity of computers, or other machines, to exhibit intelligent behaviour”. According to Niti Aayog “AI refers to the ability of machines to perform cognitive tasks like thinking, perceiving, learning, problem solving and decision making. Generative AI systems are capable of producing human-like text, images, videos, and computer code using advanced machine learning models such as large language models and deep neural networks. Generative AI systems can produce human-like text, images, videos, and computer code using advanced machine learning models. These technologies offer several benefits for education, including personalized learning, automated tutoring, and improved research support.

GENERATIVE AI IN EDUCATION

Kılıçkaya & Drgas (2025) concluded that Automated tutoring is the potential of AI but it is not to replace human tutors rather enhance traditional learning experiences, particularly through hybrid print-Augmented reality environments. Integrating AI with augmented reality can create immersive and engaging learning experiences that help reduce digital distractions. AI also improves research by making it faster and easier. It saves time and resources while simplifying data analysis. Kaswan et al (2024) deliberated that AI helps make learning more personalized by adjusting the content according to each student's needs. It allows students to study at their own speed and focus on areas where they need more improvement. Tools like intelligent tutoring systems provide specific feedback, explanations, and suggestions based on how a student interacts with the material, helping them understand concepts better and stay more engaged in the learning process.

Omar (2023) found that students using AI-driven personalized learning showed significantly higher grades and more consistent performance than those in traditional learning. Students reported that AI tools made learning more engaging through real-time feedback and personalized content (qualitative finding). Educators appreciated the analytics that helped identify students needing support, though some were concerned about over-reliance on AI and the possible loss of the human touch in teaching. Zhao et al (2025) in his study found that students with disabilities are increasingly using generative AI tools—especially chatbots, rewriting applications, and translation software—to overcome barriers in academic writing. However, concerns remain about inaccurate responses, potential academic integrity violations, and unequal access due to subscription costs. AI in education has raised significant cybersecurity concerns. Konakalla & Simuni concluded that Generative AI has the potential to significantly transform modern education. However, attention must be given to security and ethical issues to ensure its benefits are used responsibly.

However, the rapid integration of generative AI in education has raised significant cybersecurity concerns. Educational institutions manage vast digital ecosystems containing sensitive data, including student personal information, academic records, financial data, and proprietary research. This information makes schools and universities attractive targets for cybercriminals. According to cybersecurity reports, educational institutions rank among the most frequently targeted sectors for ransomware and phishing attacks.

CYBERSECURITY THREATS ASSOCIATED WITH GENERATIVE AI

Educational institutions face unique cybersecurity challenges due to their open and collaborative environments. Universities often operate large networks that support thousands of students, faculty members, and administrative staff. These networks include numerous devices, applications, and online platforms, creating multiple points of vulnerability. Cyberattacks targeting educational institutions have increased significantly in recent years. Common threats include ransomware attacks, phishing campaigns, data breaches, and unauthorized access to institutional systems. Attackers often target universities because they contain valuable research data and may have limited cybersecurity resources compared to corporate organizations.

- **Data Privacy and Information Leakage**-Generative AI raises cybersecurity concerns, especially the risk of data privacy violations when sensitive information is used in training datasets. In education, this could expose student records or other confidential data if not properly protected. To reduce these risks, institutions should use strong data protection measures such as anonymization, encryption, and strict access controls. Rijal (2024) examines This research highlights the importance of strong information security

awareness and data protection in educational institutions. It emphasizes that leadership commitment and proper employee training are key factors in maintaining effective security.

- **Cyberattacks** -Generative AI can increase cyberattack risks in educational institutions. Cybercriminals can use AI to create realistic phishing emails that appear to come from trusted sources, tricking students or staff into sharing sensitive information. AI can also generate malicious code to develop malware more quickly and efficiently. Additionally, attackers can design highly personalized social engineering messages targeting specific individuals within schools or universities, making cyberattacks more effective.
- **Deepfake and Identity Manipulation**-Deepfake technology created using generative AI poses serious risks in educational settings. Malicious individuals can create fake videos, images, or audio of students and faculty to spread misinformation, harass individuals, or damage reputations. It can also be used for identity impersonation, leading to trust issues in digital communication within institutions. As deepfakes become more realistic, it becomes harder to distinguish between real and manipulated content.
- **Academic Integrity Issues**-Generative AI creates challenges for academic integrity because students can easily generate essays, research summaries, or code, which may reduce the authenticity of their work. Traditional plagiarism tools often struggle to detect AI-generated content. To address this, institutions should introduce AI-use policies and redesigning assessments to focus on critical thinking and problem-solving skills.

GENERATIVE AI FOR CYBERSECURITY

Despite the risks associated with generative AI, these technologies also offer significant opportunities to strengthen cybersecurity in educational environments.

- **Threat Detection**-Generative AI can analyse large volumes of network data to identify unusual patterns and potential security threats. AI can keep check on educational networks and quickly detect unusual activities or potential cyberattacks on LMS, digital Classrooms. Machine learning algorithms can detect anomalies in network traffic, user behaviour, and system activity. By identifying suspicious activities early, AI-powered security systems can help institutions respond quickly to cyber incidents and prevent large-scale breaches. AI systems can identify and block phishing emails targeting students and staff. AI can analyse files and systems to detect and prevent malware or ransomware attacks.
- **Education and Training**-Generative AI can also enhance cybersecurity education by creating realistic training environments. AI-based simulations can replicate cyberattack scenarios, allowing students to practice defending systems against threats. These simulations provide hands-on learning experiences in areas such as ethical hacking, malware analysis, and digital forensics. Such training prepares students for careers in cybersecurity and strengthens the overall security workforce.
- **Security Management**-AI-powered tools can automate routine cybersecurity tasks such as vulnerability scanning, incident detection, and security monitoring. Automation reduces the workload of IT security teams and allows them to focus on more complex threats. AI helps educational institutions monitor their digital systems continuously without requiring constant human supervision. In addition, AI systems can continuously

monitor institutional networks, ensuring that potential vulnerabilities are identified and addressed promptly. AI helps secure sensitive student and institutional data through advanced encryption and anomaly detection.

POLICY FRAMEWORK FOR USE OF GENERATIVE AI

- **AI Usage Policies-** Institutions should establish clear guidelines regarding the acceptable use of generative AI tools.
- **Data Protection Measures-** Educational organizations must implement strong data protection strategies to safeguard sensitive information. These measures include encryption, secure authentication systems, and restricted access to confidential datasets.
- **Cybersecurity Awareness Programs-** Seminars and workshops should be organized in institutions for training faculty and staff on usage of AI and various issues of Cybersecurity.

CONCLUSION

Publicly available generative AI tools are developing very quickly, and new versions are being released faster than national regulations can adapt. In many countries, the lack of clear regulations leaves users' data privacy insufficiently protected and makes it difficult for educational institutions to properly evaluate and regulate these tools. AI in education will depend on balancing innovation with security. By adopting comprehensive policies, promoting digital literacy, and strengthening cybersecurity infrastructure, educational institutions can harness the benefits of generative AI while minimizing potential risks.

REFERENCES

1. Holmes, W., Miao, F., & Unesco. (2023). Guidance for generative AI in Education and Research. UNESCO Publishing. <https://www.unicef.org/innocenti/can-ai-help-bridge-gap-inclusive-education>
2. Jian, M. J. K. O. (2023). Personalized learning through AI. *Advances in Engineering Innovation*, 5(1), 16–19. <https://doi.org/10.54254/2977-3903/5/2023039>
3. Kılıçkaya, F., Kic-Drgas, J. The future of tutoring: AI as an augmenting force. *AI & Soc* 40, 6489–6490 (2025). <https://doi.org/10.1007/s00146-025-02356-0>
4. Konakalla, P. K., & Simuni, G. (n.d.). Security and privacy concerns in Generative AI [Thesis].
5. Rijal, D. M., Assydiqi, M. F., Prasetya, Y. R., Ningsih, L. N. P., Anindra, N. K. P., & Pambudi, P. D. L. (2024). Information security awareness analysis of the threat of data leakage in educational institutions with the ISO 27001 framework. *Journal of Digital Business and Innovation Management*, 3(1), 36–52. <https://doi.org/10.26740/jdbim.v3i1.59167>
6. Singh Kaswan, K., Singh Dhatteval, J., & Ojha, R. P. (2024). AI in personalized learning. In *Advances in Technological Innovations in Higher Education* (1st Edition, p. 15). CRC Press.
7. Zhao, X., Cox, A., & Chen, X. (2025). The use of generative AI by students with disabilities in higher education. *The Internet and Higher Education*, 66, 101014. <https://doi.org/10.1016/j.iheduc.2025.101014>