GYANBODH
An International Multidisciplinary Peer Reviewed Journal
ISSN:3048-9792
Volume: 3
Issue: 2
Special Issue: 1
May: 2026

# Learning in the Digital Age: Cyber Security Risks and Opportunities of ICT and AI for Students

Dr. Lata Pandey
Assistant Professor
Department of Education (CASE), The Maharaja Sayajirao University of Baroda
lata.pandey-edu@msubaroda.ac.in,
7573007480(Calling No.), 9685287978(WhatsApp No.)

**Abstract**

In the digital age, Information and Communication Technology (ICT) and Artificial Intelligence (AI) have revolutionized educational landscapes, offering personalized learning experiences and enhanced accessibility for students. However, this integration introduces significant cyber security risks, including data breaches, phishing attacks, and AI-driven vulnerabilities such as prompt injection and data poisoning. Conversely, opportunities arise from AI's capacity for real-time threat detection, automated incident response, and innovative teaching tools that bolster cyber defense skills. This paper examines these dual aspects, drawing on recent studies and discussions to highlight how educational institutions can mitigate risks while capitalizing on opportunities. By addressing data governance, ethical AI use, and proactive security measures, stakeholders can create safer digital learning environments. The study concludes that a balanced and informed approach is necessary to ensure secure, ethical, and effective use of digital technologies in education.

## Introduction

The rapid proliferation of Information and Communication Technology (ICT) and Artificial Intelligence (AI) in education has ushered in a new era of dynamic, personalized, and inclusive learning experiences. Students now benefit from AI-powered tutors, adaptive learning platforms, and vast online resources that foster interactivity, collaboration, and individualized instruction, enabling greater access to education and skill development for diverse learners (UNESCO, 2025; Intel, 2025). These technologies enhance student engagement through intelligent tutoring systems, automated feedback, and data-driven insights that tailor content to individual needs, while also streamlining administrative tasks for educators (Hooshyar et al., 2023; Whalley et al., 2021).

GYANBODH
An International Multidisciplinary Peer Reviewed Journal
ISSN:3048-9792
Volume: 3
Issue: 2
Special Issue: 1
May: 2026

However, this digital transformation significantly heightens cybersecurity vulnerabilities, positioning the education sector as a prime target for cybercriminals due to its wealth of sensitive student data and often limited resources. In 2025, educational institutions worldwide faced an alarming surge in attacks, becoming the most targeted industry with an average of over 4,300 weekly cyberattacks per organization in some periods—a stark increase driven by ransomware, phishing, and data breaches (Deepstrike, 2025; Check Point Research, 2025). In the U.S., 82% of K-12 schools reported experiencing a cyber incident between July 2023 and December 2024, underscoring the pervasive threats that disrupt learning, compromise privacy, and incur substantial financial costs (Center for Internet Security, 2025).

This paper examines the dual-edged nature of ICT and AI integration in education, analyzing key cybersecurity risks—such as data breaches, AI-amplified phishing and ransomware, prompt injection vulnerabilities, and ethical concerns like bias and over-dependence—alongside the substantial opportunities for enhanced learning outcomes, equity, and innovation. By providing evidence-based insights and recommendations, it aims to guide educators, policymakers, and institutions in developing balanced strategies that maximize benefits while implementing robust safeguards to protect students in the digital age.

**Rationale of the Study**

The unprecedented pace of ICT and AI adoption in education has created a pressing need for research that simultaneously examines their transformative benefits and emerging cybersecurity challenges. While numerous studies highlight the advantages of personalized learning and AI-driven tools, and others focus on general cyber threats, few integrate these dimensions specifically for student populations in the current digital landscape (UNESCO, 2025; Gerlich, 2025). With the education sector now ranking as the most attacked industry globally in 2025—facing over 4,300 weekly cyberattacks per organization and a sharp rise in AI-enhanced threats—this study fills a critical gap by providing a holistic, student-centered analysis of risks and opportunities (Check Point Research, 2025; Deepstrike, 2025).

**Significance of the Study**

This paper is highly significant as it illuminates the double-edged impact of digital technologies in education: empowering students with innovative, inclusive, and adaptive learning experiences while exposing them to severe cybersecurity vulnerabilities that can undermine

GYANBODH
An International Multidisciplinary Peer Reviewed Journal
ISSN:3048-9792
Volume: 3
Issue: 2
Special Issue: 1
May: 2026

privacy, trust, and academic continuity. At a time when 86% of educational institutions actively deploy generative AI and ransomware attacks on schools increased dramatically—with 180 incidents recorded worldwide through Q3 2025—the findings offer timely, evidence-based guidance for educators, administrators, and policymakers (Microsoft, 2025; Comparitech, 2025). By balancing opportunities with practical risk mitigation strategies, this work contributes to building resilient, equitable, and secure digital learning ecosystems that prepare students safely for the future.

**Research Objectives**

1. To identify and analyze the key cyber security risks posed by ICT and AI to students in digital learning settings.
2. To explore the opportunities that ICT and AI provide for enhancing cyber security and educational outcomes.
3. To propose recommendations for mitigating identified risks while maximizing opportunities to promote secure and effective digital education.

**Cyber Security Risks of ICT and AI for Students**

The integration of Information and Communication Technology (ICT) and Artificial Intelligence (AI) in education has transformed learning but also heightened cybersecurity vulnerabilities for students. In 2025, the education sector became the most targeted industry for cyberattacks worldwide, experiencing an average of over 4,300 weekly attacks per organization—a significant increase from prior years (Check Point Research, 2025; Deepstrike, 2025). Primary risks include data breaches exposing sensitive student information, such as personal details, academic records, and biometric data, often leading to identity theft, reputational harm, and financial losses. For example, major incidents like the PowerSchool breach affected millions of students and teachers, highlighting vulnerabilities in learning management systems (LMS) (Comparitech, 2025).

In eLearning platforms, phishing and ransomware threats are prevalent and increasingly sophisticated due to AI enhancements. Phishing remains a dominant vector, with AI enabling hyper-personalized, error-free deceptive emails that exploit trust. Ransomware attacks on education rose 23% year-over-year in the first half of 2025, with 130 incidents reported and average demands exceeding $550,000 (Comparitech, 2025). Globally, 180 ransomware attacks

GYANBODH
An International Multidisciplinary Peer Reviewed Journal
ISSN:3048-9792
Volume: 3
Issue: 2
Special Issue: 1
May: 2026

hit the sector in the first three quarters of 2025 (K-12 Dive, 2025). AI amplifies these by generating convincing deepfakes or automated campaigns, making detection harder.

AI-specific vulnerabilities, such as prompt injection in educational chatbots and tools, allow attackers to manipulate systems by embedding malicious instructions, leading to data leaks or harmful outputs. Ranked as the top LLM risk in 2025 by OWASP, prompt injection exploits the inability of models to distinguish trusted instructions from user input (OWASP Gen AI Security Project, 2025).

Finally, cognitive and ethical risks emerge from over-dependence on AI, potentially diminishing students' critical thinking, decision-making, and analytical skills. Studies show heavy AI reliance correlates with lower critical thinking scores, mediated by cognitive offloading where mental effort is reduced (Gerlich, 2025; Zhai et al., 2024). Approximately 27-30% of students exhibit degraded higher-order thinking due to this dependency, alongside concerns over biases perpetuating inequalities (Phys.org, 2025; Springer, 2024).

**Opportunities of ICT and AI in Education for Cyber Security**

The integration of Information and Communication Technology (ICT) and Artificial Intelligence (AI) in education offers transformative opportunities to strengthen cybersecurity awareness, training, and skill development among students. AI-powered tools enable interactive simulations, personalized learning paths, and real-time feedback in hands-on labs, making complex cybersecurity concepts more accessible and practical (SIGCSE, 2025; EdTech Magazine, 2025). For instance, AI-driven platforms create adaptive phishing simulations and gamified scenarios that mirror real-world threats, enhancing student engagement and retention while teaching threat recognition and response (EdTech Magazine, 2025; ResearchGate, 2024). Additionally, initiatives like student-operated Security Operations Centers (SOCs) and AI-augmented curricula prepare learners for emerging careers, with growing interest in AI and cybersecurity pathways in career and technical education (CTE) programs (GovTech, 2025; Cool Cat Teacher, 2025). Global efforts, such as IBM's commitment to skill millions in AI and cybersecurity, further democratize access to advanced training, fostering ethical awareness, critical thinking, and workforce readiness in an AI-driven threat landscape (IBM, 2025).

By leveraging ICT platforms for collaborative tools and AI for predictive analytics and automated assessments, educational institutions can cultivate a proactive culture of digital

GYANBODH
An International Multidisciplinary Peer Reviewed Journal
ISSN:3048-9792
Volume: 3
Issue: 2
Special Issue: 1
May: 2026

resilience, equipping students not only to defend against threats but also to innovate in cybersecurity fields (DeVry University, 2025; NSF, 2025).

**Recommendations for Mitigating Risks and Maximizing Opportunities**

To navigate the dual-edged nature of ICT and AI in education, institutions must adopt proactive, multifaceted strategies grounded in best practices and ethical guidelines (CISA, 2025; U.S. Department of Education, 2025). Key recommendations include:

1. **Strengthen Cybersecurity Infrastructure:** Implement Zero Trust Architecture, multi-factor authentication (MFA), network segmentation, and regular software updates to minimize vulnerabilities. Adopt frameworks like the NIST Cybersecurity Framework or CISA's K-12 guidelines for systematic risk management (NIST, 2025; CISA, 2025).
2. **Promote Cybersecurity Awareness and Training:** Conduct ongoing training for students, teachers, and staff on recognizing phishing, safe AI use, and cyber hygiene. Integrate AI literacy and ethical considerations into curricula, including simulations for prompt injection and bias detection (TeachAI, 2025; CoSN, 2025).
3. **Develop Clear AI Governance Policies:** Create school-specific AI guidance covering data privacy, ethical use, academic integrity, and security evaluations of tools. Ensure compliance with laws like FERPA and COPPA, and involve stakeholders in policy development (U.S. Department of Education, 2025; Georgia Department of Education, 2025).
4. **Leverage AI for Defense:** Use AI-driven tools for threat detection, automated incident response, and behavioral analytics to enhance protection while teaching students responsible AI applications (DeVry University, 2025; Center for Internet Security, 2025).
5. **Foster Collaboration and Continuous Monitoring:** Partner with federal resources, industry experts, and other institutions for threat intelligence sharing. Regularly audit AI systems and conduct incident response planning to build resilience (SchoolSafety.gov, 2025).

By implementing these measures, educational institutions can harness ICT and AI's potential while safeguarding students in an evolving digital landscape.

GYANBODH
An International Multidisciplinary Peer Reviewed Journal
ISSN:3048-9792
Volume: 3
Issue: 2
Special Issue: 1
May: 2026

## Conclusion

The integration of ICT and AI in education represents a profound opportunity to revolutionize learning, making it more personalized, accessible, and engaging while simultaneously equipping students with essential cybersecurity skills for the future. However, as evidenced throughout this paper, these technologies introduce substantial risks—ranging from escalated data breaches and AI-amplified attacks to ethical dilemmas like bias and cognitive over-dependence—that have positioned the education sector as the most vulnerable to cyberattacks in 2025.

Ultimately, the path forward lies in a balanced, proactive approach: embracing innovation while prioritizing robust safeguards, ethical governance, and comprehensive training. By adopting the recommended strategies, educators, policymakers, and institutions can mitigate threats, maximize opportunities, and cultivate secure, resilient digital learning environments. In doing so, we not only protect students today but also empower them to thrive in an AI-driven world tomorrow, ensuring that technology serves as a force for equitable and safe educational advancement.

## References

Center for Internet Security. (2025). *2025 CIS MS-ISAC K-12 cybersecurity report: Where education meets community resilience*. https://www.cisecurity.org/insights/white-papers/2025-k12-cybersecurity-report

Check Point Research. (2025). *Q1 2025 global cyber attack report*. Check Point Software Technologies. https://blog.checkpoint.com/research/q1-2025-global-cyber-attack-report-from-check-point-software-an-almost-50-surge-in-cyber-threats-worldwide-with-a-rise-of-126-in-ransomware-attacks/

Comparitech. (2025). *Education ransomware roundup: Q1-Q3 2025 stats on attacks, ransoms, and data breaches*. https://www.comparitech.com/news/education-ransomware-roundup-q1-q3-2025-stats-on-attacks-ransoms-and-data-breaches/

Cybersecurity and Infrastructure Security Agency. (2025). *Cybersecurity best practices for K-12*. U.S. Department of Homeland Security. https://www.cisa.gov/topics/cybersecurity-best-practices/K12cybersecurity

GYANBODH
An International Multidisciplinary Peer Reviewed Journal
ISSN:3048-9792
Volume: 3
Issue: 2
Special Issue: 1
May: 2026

Deepstrike. (2025). *Data breaches in education 2025: The growing cybersecurity crisis*. https://deepstrike.io/blog/data-breaches-education-2025

DeVry University. (2025). *The future of AI and cybersecurity: How educational institutions are poised for 2025 and beyond*. https://www.devry.edu/newsroom/news/2025/the-future-of-ai-and-cybersecurity-how-educational-institutions-are-poised-for-2025-and-beyond.html

EdTech Magazine. (2025). *How schools can prepare for artificial intelligence-backed cyberattacks*. https://edtechmagazine.com/k12/article/2025/03/how-schools-can-prepare-artificial-intelligence-backed-cyberattacks

Gerlich, M. (2025). AI tools in society: Impacts on cognitive offloading and the future of critical thinking. *Societies, 15*(1), Article 6. https://doi.org/10.3390/soc15010006

GovTech. (2025). *CTE students increasingly interested in AI, IT, cybersecurity*. https://www.govtech.com/education/k-12/cte-students-increasingly-interested-in-ai-it-cybersecurity

IBM. (2025). *IBM commits to skill 5 million Indian youth in AI, cybersecurity & quantum by 2030*. https://in.newsroom.ibm.com/2025-12-19-IBM-commits-to-skill-5-million-Indian-youth-in-AI%2C-Cybersecurity-Quantum-by-2030

Intel. (2025). *Artificial intelligence in education*. https://www.intel.com/content/www/us/en/learn/ai-in-education.html

K-12 Dive. (2025). *180 ransomware attacks plague education sector worldwide in 2025 through Q3*. https://www.k12dive.com/news/first-dip-ransomware-attacks-quarters-since-2024-comparitech/804339/

Microsoft. (2025). *2025 AI in education report*. https://www.microsoft.com/en-us/education/2025-ai-in-education-report

National Science Foundation. (2025). *Cybersecurity education in the age of artificial intelligence*. https://www.nsf.gov/funding/opportunities/dcl-cybersecurity-education-age-artificial-intelligence/nsf20-072

OWASP Gen AI Security Project. (2025). *OWASP top 10 for LLM applications 2025*. https://genai.owasp.org/resource/owasp-top-10-for-llm-applications-2025/

GYANBODH
An International Multidisciplinary Peer Reviewed Journal
ISSN:3048-9792
Volume: 3
Issue: 2
Special Issue: 1
May: 2026

ResearchGate. (2024). *Innovating cybersecurity education through AI-augmented teaching*. https://www.researchgate.net/publication/381651850_Innovating_Cybersecurity_Education_Through_AI-augmented_Teaching

SIGCSE. (2025). *Enhancing cybersecurity education with artificial intelligence content*. https://sigcse2025.sigcse.org/details/sigcse-ts-2025-Papers/160/Enhancing-Cybersecurity-Education-with-Artificial-Intelligence-Content

U.S. Department of Education. (2025). *Guidance on artificial intelligence use in schools*. https://www.ed.gov/about/news/press-release/us-department-of-education-issues-guidance-artificial-intelligence-use-schools

UNESCO. (2025). *Artificial intelligence in education*. https://www.unesco.org/en/digital-education/artificial-intelligence

Zhai, C., Wibowo, S., & Li, L. D. (2024). The effects of over-reliance on AI dialogue systems on students' cognitive abilities: A systematic review. *Smart Learning Environments, 11*, Article 28. https://doi.org/10.1186/s40561-024-00316-7