Strengthening the Role of Cyber Security for Students in Addressing Information Security Threats in the Era of Artificial Intelligence

Taufik Iqbal Ramdhani[1]*, Dwi Utari Iswavigra[2], Deny Prasetyo[2], Yulaikha M[2], Ardy Wicaksono[2], Suyahman[2]*

[1]Research Center for Artificial Intelligence and Cyber Security, National Research and Innovation of Agency, Bandung, Indonesia
[2,]Department of Computer Science, Universitas Sugeng Hartono, Sukoharjo, Indonesia

Abstract. The rapid development of Artificial Intelligence (AI) has significantly transformed digital ecosystems, bringing both opportunities and challenges, particularly in the field of information security. While AI enhances efficiency and innovation, it also increases vulnerability to cyber threats such as data breaches, phishing, malware, and social engineering. Students, as active users of digital technologies and AI-based applications, are among the most exposed groups to these risks. Therefore, strengthening the role of cyber security is essential to improve students' awareness and ability to address emerging information security threats. This community service activity aimed to strengthen the role of cyber security for students in the era of Artificial Intelligence through an educational and participatory approach. The activity was conducted using a hybrid seminar model involving 48 undergraduate students from Universitas Sugeng Hartono. The offline session took place in Room 15 of the university campus in Solo Baru, Sukoharjo, Central Java, while the speaker delivered the material online via Zoom on Thursday, January 29, 2026. The results indicate that the activity successfully increased students' understanding of AI and cyber security, improved their awareness of data privacy risks, and encouraged more proactive attitudes toward digital security practices. Students demonstrated high enthusiasm and active participation during discussions. Overall, the program proved effective in enhancing cyber security awareness and preparing students to face information security threats in the era of Artificial Intelligence.

Keywords: Cyber Security, Information Security, Artificial Intelligence, Student Awareness, Digital Literacy
Received January 2026 / **Revised** February 2026 / **Accepted** February 2026

INTRODUCTION

Rapid digital advancements transform education, industry, and public services fundamentally. Artificial Intelligence drives this change through automation and complex data analysis across various sectors [1]. These systems simplify decision-making by integrating intelligent algorithms into daily operations. However, widespread adoption requires a deep understanding of system mechanisms to ensure optimal benefits.

Artificial Intelligence now moves beyond research laboratories and into common digital applications. The educational sector utilizes these technologies for learning management and automated grading [2]. Students frequently employ generative tools to assist with their academic assignments. This integration creates an adaptive learning environment that relies heavily on digital infrastructure.

Digital data volumes grow at an exponential rate as users interact more frequently with technology. This data explosion includes personal records, academic history, and institutional information stored in global networks [3]. Such a phenomenon creates massive information pools managed through various online platforms. Consequently, reliance on cloud storage and data transmission becomes an unavoidable reality.

Large-scale data availability supports the effectiveness of Artificial Intelligence systems. On the other hand, this creates significant information security vulnerabilities. Integrating AI into digital ecosystems expands the attack surface for cyber threats [4]. Data becomes susceptible to unauthorized access, manipulation, and damaging leaks.

[1]*Corresponding author.
Email addresses: suyahman@sugenghartono.ac.id (Suyahman)

Information security aims to protect data from threats that compromise system confidentiality and availability. Cyber security serves as the primary defense against malicious activities within digital networks. The main focus involves closing system vulnerabilities to ensure consistent data protection [5]. This effort requires coordination between robust technology and strict procedural standards.

The relationship between Artificial Intelligence and cyber security remains highly complex. AI technology strengthens defenses through intelligent threat detection and automated anomaly analysis. Conversely, attackers exploit similar technologies to create adaptive and evasive attack methods [6]. This dynamic creates a technological race between defense systems and offensive strategies.

Modern cyber threats evolve far beyond traditional hacking or simple viruses. New forms of attacks include deepfake-based fraud and social engineering supported by AI algorithms [7]. Automated malware now adapts to target environments to bypass security software effectively. These shifts demand constant updates to data protection strategies.

Students represent one of the most active groups of digital technology users. Online platforms serve as their primary tools for daily learning, collaboration, and communication. High digital interaction leaves students highly exposed to various cyber security risks [8]. A lack of awareness regarding information security practices often worsens their vulnerability online.

Many students demonstrate limited understanding of core cyber security concepts. They often underestimate the risks of weak passwords or insecure network connections. Such negligence leads to serious consequences like identity theft or the loss of critical academic data [9]. Practical awareness remains the key to minimizing the negative impacts of digital activities.

The availability of generative AI tools increases the complexity of security risks for students. Many utilize these applications without considering data privacy or intellectual property issues. A focus on instant results often ignores ethical usage and the security of the systems involved [10]. This ignorance creates new challenges for academic integrity within university environments.

This situation emphasizes the urgent need for systematic cyber security education programs. Such education must go beyond mere technical knowledge. Critical awareness of information risks and responsible digital behavior must form the core of the curriculum [11]. Does the current educational framework address these evolving threats fast enough? Comprehensive programs must be implemented immediately to answer this challenge.

Strengthening cyber security roles among students serves as a crucial preventive strategy. Improved literacy helps students identify potential threats early in their digital interactions [12]. Security-conscious students can protect their personal data independently while using modern technology. This also encourages the ethical and safe use of Artificial Intelligence.

Universities hold a strategic role in promoting digital literacy to the broader community. Educational institutions bear the responsibility of equipping students with practical navigation skills for the digital world. Beyond academic knowledge, cyber risk protection becomes a mandatory competency for future graduates [13]. These efforts support the creation of a healthier and more protected digital ecosystem.

This study focuses on strengthening cyber security awareness for students in the AI era [14]. Education delivered through a hybrid seminar model enhances student readiness against evolving cyber risks [15]. The primary objective involves providing a deep understanding of modern digital threat mechanisms. This step ensures that the transition into a digital era remains secure [16].

METHODS

This community service activity employs an educational and participatory approach to strengthen student understanding of cyber security within the context of Artificial Intelligence [17]. As seen in Figure 1, the process begins with preparation and continues with observation and reflection to gauge student understanding.

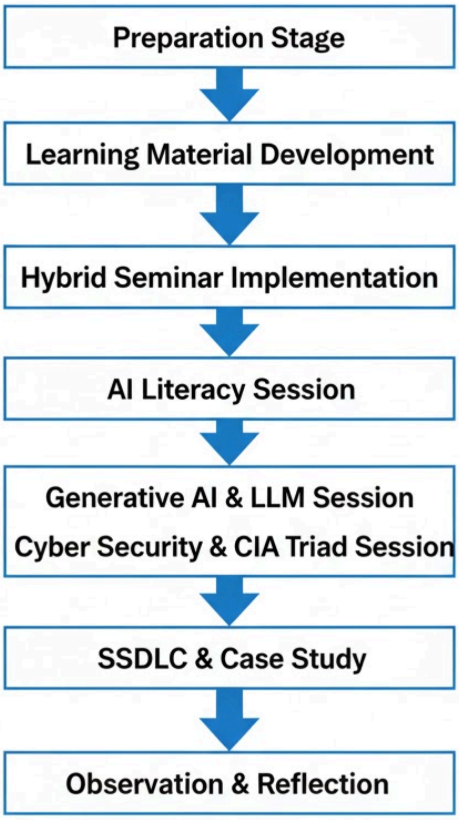
Preparation Stage
Learning Material Development
Hybrid Seminar Implementation
AI Literacy Session
Generative AI & LLM Session
Cyber Security & CIA Triad Session
SSDLC & Case Study
Observation & Reflection

Figure 1. Learning Stage

The design includes a seminar and interactive discussion to provide theoretical knowledge alongside practical insights into digital information threats. This structure facilitates a comprehensive learning environment for all participants. The learning materials provided can be seen in Table 1.

Table 1. Learning Materials

Session	Main Topic	Learning Objectives
1	Data Explosion	Understanding exponential data growth and its security implications
2	Foundations of AI	Introducing AI, ML, and DL concepts
3	Generative AI & LLM	Understanding generative AI, GPT, and risks of data misuse
4	Cyber Security Fundamentals	Introducing cyber threats and attack types
5	CIA Triad & PPT	Understanding confidentiality, integrity, availability
6	SSDLC	Understanding security in software development
7	Case Studies	Analyzing real-world cyber attacks
8	Ethical AI Usage	Promoting responsible AI practices

The learning sessions follow a systematic organization divided into eight main topics to provide a comprehensive understanding of Artificial Intelligence and cyber security. The first session addresses the phenomenon of Data Explosion, helping students grasp the exponential growth of digital data and its security implications. The second session introduces the Foundations of Artificial Intelligence by covering core concepts of Machine Learning and Deep Learning. These topics serve as the theoretical basis for all subsequent technical discussions [18].

The third session focuses on Generative AI and Large Language Models (LLM) to explain how models like GPT function. This segment emphasizes potential risks such as data misuse and privacy leakage in academic and professional settings [19]. In the fourth session, the curriculum shifts to Cyber Security

Fundamentals, providing an overview of common cyber threats and modern attack types. This foundational knowledge allows students to identify vulnerabilities in the digital environment [20].

The fifth session explains the core principles of information security through the CIA Triad and the People, Processes, and Technology (PPT) framework. This session highlights the necessity of maintaining confidentiality, integrity, and availability in every digital system [21]. The sixth session introduces the Secure Software Development Life Cycle (SSDLC) to demonstrate how security must be integrated into the software development process [22].

Practical understanding is enhanced in the seventh session through the presentation of real-world Case Studies of cyber attacks. By analyzing actual incidents, students can better understand the consequences of security failures [23]. Finally, the eighth session promotes Ethical AI Usage to encourage responsible and safe practices among technology users. This concluding topic ensures that students apply their technical skills within an ethical and legal framework [24].

The participant group consists of 48 undergraduate students from Universitas Sugeng Hartono. These students represent various academic backgrounds and use digital technologies and AI-based applications extensively in their daily tasks. Researchers selected this specific group due to their high level of interaction with modern digital platforms.

The activity took place on Thursday, January 29, 2026, at Room 15 on the Universitas Sugeng Hartono Campus in Solo Baru, Sukoharjo. The implementation utilizes a hybrid model where students gather offline in a classroom while the speaker presents through the Zoom platform. This setup bridges physical presence with digital communication tools effectively.

Choosing a hybrid learning model optimizes accessibility and flexibility for the invited speakers and students [25]. This approach reflects the actual context of modern digital learning environments while supporting the objective of introducing cyber security awareness. It allows for direct interaction through digital interfaces, mimicking common professional and academic settings.

Delivery methods include lectures, case studies, and interactive discussions to engage the participants. The lecture session explains fundamental concepts of Artificial Intelligence and information security threats. Meanwhile, specific case studies illustrate real-world cyber incidents and the potential risks linked to the misuse of AI technologies.

Qualitative methods serve as the primary tool for evaluating the effectiveness of this activity. Assessment focuses on direct observation of student participation and engagement levels during the discussion segments. Indicators such as student enthusiasm and the depth of the questions raised help determine the success of the program [26].

RESULT AND DISCUSSION

The community service activity concluded successfully with 48 undergraduate students from Universitas Sugeng Hartono participating in the session. This hybrid seminar model allowed students to gather in a physical classroom while interacting with the speaker through an online platform. The activity proceeded smoothly and met all predefined objectives according to the initial plan.

Direct observations during the session revealed a high level of enthusiasm toward the intersection of Artificial Intelligence and cyber security. Students remained attentive throughout the presentation and actively took notes on key concepts. This engagement translated into a willingness to participate in deep discussions regarding information security issues.

Before the intervention, most participants possessed a limited conceptual understanding of Artificial Intelligence beyond its basic applications. Many viewed these technologies strictly as academic assistance tools. Consequently, they often failed to recognize the broader implications for data privacy, security risks, and significant ethical challenges. The results of the intervention can be seen in Table 2.

Post-activity assessments showed that students gained a clearer understanding of the role AI plays within digital systems. Participants identified how these systems collect and process massive data volumes, which heightens vulnerability to cyber threats. This realization highlighted the necessity of implementing robust protection measures for personal and institutional information.

Table 2. Intervention Results

Aspect of Literacy	Before the Activity	After the Activity
Understanding of Artificial Intelligence	Low	Improved
Awareness of data privacy risks	Low	High
Knowledge of cyber threats	Limited	Broader
Attitude toward information security	Passive	More proactive
Participation in discussions	Low	High
Understanding of ethical AI use	Limited	Improved

The interactive discussion revealed that students previously underestimated common cyber security risks in their daily digital routines. Many considered practices like using weak passwords or accessing public Wi-Fi networks to be normal and harmless. Such behavior stems from a lack of exposure to the potential consequences of data exposure in online environments.

Following the educational intervention, awareness of specific threats such as phishing, malware, and social engineering increased significantly. Students learned how AI-driven attacks can amplify these threats through automated messaging and deepfake technology. Understanding these sophisticated methods allows for better preparation against modern digital fraud.

One significant outcome involved a shift in student attitudes toward protecting digital identities. Participants expressed a more proactive stance by committing to stronger passwords and enabling two-factor authentication. They also showed greater caution when interacting with unknown digital sources or unverified platforms.

The integration of real-world case studies improved the overall learning experience by grounding theoretical concepts in practical reality. Analyzing actual cyber incidents helped students relate academic information to tangible risks they might encounter. This approach made the complex subject matter more meaningful and relevant to their lives.

From an educational perspective, the hybrid learning model functioned effectively for delivering cyber security awareness. The combination of offline presence and online communication maintained high engagement levels while providing flexibility for the guest speaker. This format successfully bridged the gap between different learning environments.

The results indicate that this activity contributed positively to strengthening cyber security awareness among the student body. Improvements in knowledge and attitude demonstrate that educational interventions remain essential for preparing individuals for the AI era. Such programs build the necessary resilience against evolving information security threats. Documentation of the activity can be seen in Figure 2.

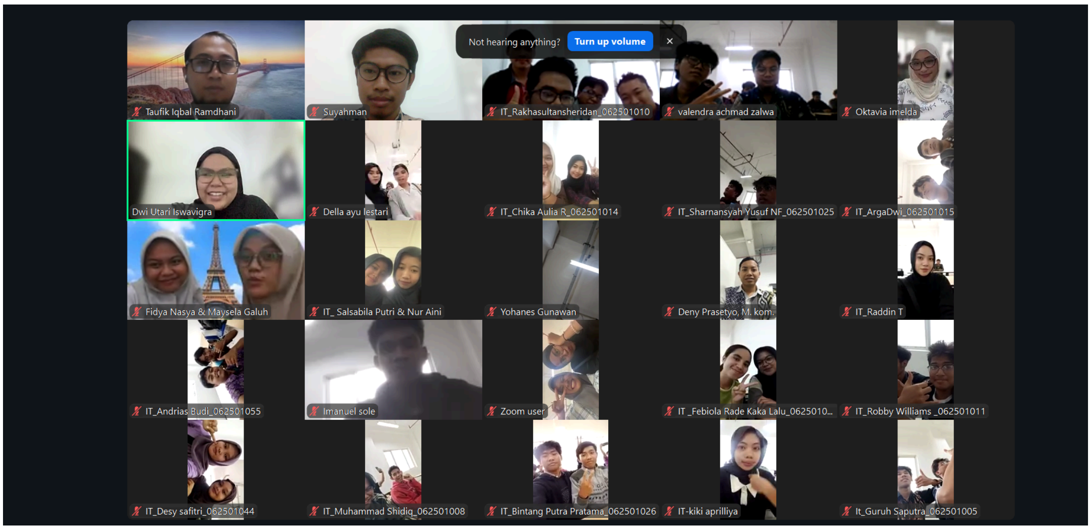
Not hearing anything?
Turn up volume
Taufik Iqbal Ramdhani
Suyahman
IT_Rakhasultansheridan_062501010
valendra achmad zalwa
Oktavia imelda
Dwi Utari Iswavigra
Della ayu lestari
IT_Chika Aulia R_062501014
IT_Sharnansyah Yusuf NF_062501025
IT_ArgaDwi_062501015
Fidya Nasya & Maysela Galuh
IT_ Salsabila Putri & Nur Aini
Yohanes Gunawan
Deny Prasetyo, M. kom.
IT_Raddin T
IT_Andrias Budi_062501055
Imanuel sole
Zoom user
IT _Febiola Rade Kaka Lalu_0625010...
IT_Robby Williams _062501011
IT_Desy safitri_062501044
IT_Muhammad Shidiq_062501008
IT_Bintang Putra Pratama_062501026
IT-kiki aprilliya
It_Guruh Saputra_062501005

Figure 2. Documentation of the activity

CONCLUSION

The community service activity served to strengthen the role of cyber security for students facing information security threats in the era of Artificial Intelligence. The implementation used a hybrid seminar model involving 48 undergraduate students from Universitas Sugeng Hartono. This format combined offline classroom attendance with online expert delivery to bridge geographical gaps. The program provided fundamental knowledge and practical insights into the intersection of AI and modern cyber security. Results indicate that the activity improved student understanding, awareness, and attitudes toward information security. Participants became more conscious of risks associated with digital technologies and the potential misuse of AI. They also recognized the critical importance of protecting personal data and maintaining secure digital practices. This educational approach effectively strengthened student readiness to face emerging threats in the digital environment. In conclusion, strengthening cyber security awareness through educational programs remains essential in the era of Artificial Intelligence. Universities should integrate cyber security literacy into academic and extracurricular activities regularly. Such initiatives ensure that students remain technologically skilled while using digital tools safely, responsibly, and ethically. Continuous education provides the best defense against the rapid evolution of digital risks.

REFERENCES

[1] T. H. Le, "Digital transformation: Artificial intelligence shaping the future of public sector," New Applied Studies in Management, Economics & Accounting, vol. 7, no. 1, hlm. 43–52, Mar. 2024.

[2] A. M. Alenezi, "Generative artificial intelligence (AI) in higher education: A comprehensive review of challenges, opportunities, and implications," Journal of Learning Development in Higher Education, no. 30, hlm. 1–24, Mar. 2024.

[3] S. Chilakala, "Enterprise Data Architectures: A Comprehensive Analysis of Modern Solutions, Market Trends, and Implementation Frameworks," International Journal of Research in Computer Applications and Information Technology, vol. 8, no. 1, hlm. 1–15, Jan. 2025.

[4] J. A. O. Alie et al., "AI and cybersecurity: A risk society perspective," Frontiers in Sociology, vol. 9, hlm. 1–14, Okt. 2024.

[5] E. D. V. P. Cardenas, "Building a Cybersecurity Culture in Higher Education: Proposing a Cybersecurity Awareness Paradigm," Applied Sciences, vol. 14, no. 3, hlm. 1–18, Feb. 2024.

[6] S. K. Mamillapalli, "Adversarial and Offensive AI in Cyber Security," International Journal on Science and Technology, vol. 15, no. 4, hlm. 1–8, Des. 2024.

[7] F. M. Alotaibi, "Deepfake-Driven Social Engineering: Threats, Detection Techniques, and Defensive Strategies in Corporate Environments," Encyclopedia, vol. 4, no. 4, hlm. 1–16, Nov. 2024.

[8] R. B. Santelices, "A Students' Perspective on Cybersecurity Awareness and Education," International Journal of Research and Innovation in Social Science, vol. 9, no. 11, hlm. 550–562, Nov. 2025.

[9] M. H. M. A. Sampa dan M. K. Mahmud, "Factors Affecting Cybersecurity Awareness among University Students," Journal of Information Systems and Informatics, vol. 5, no. 1, hlm. 120–133, Mar. 2023.

[10] T. S. M. T. S. Binti, "Generative AI and Academic Integrity in Higher Education: A Systematic Review and Research Agenda," Education Sciences, vol. 14, no. 6, hlm. 1–20, Jun. 2024.

[11] R. Lawrence et al., "Developing a Cybersecurity Curriculum Using Best Practices and Student Awareness Insights," The Journal of Computational Science Education, vol. 14, no. 1, hlm. 34–45, Nov. 2023.

[12] H. Saputra, "Digital Literacy as a Cyber Crime Defense and Prevention Strategy," International Journal of Latest Technology in Engineering Management & Applied Science, vol. 14, no. 9, hlm. 45–56, Sep. 2025.

[13] M. Prakasha et al., "Digital Security in Educational Contexts: Digital Competence and Challenges for Good Practice," European Journal of Education, vol. 59, no. 3, hlm. 102–118, Agu. 2024.

[14] A. F. S. Ardhiyasa dan D. Syamsuar, "Comprehensive Analysis of Cybersecurity Awareness Among Students' Universities," International Journal of Innovative Technology and Exploring Engineering, vol. 14, no. 5, hlm. 12–20, Apr. 2025.

[15] K. A. Kee et al., "Hybrid learning in post-pandemic higher education systems: An analysis using SEM and DNN," Journal of Applied Research in Higher Education, vol. 17, no. 1, hlm. 101–123, Feb. 2025.

[16] N. T. Van et al., "Assessing student readiness for mobile learning from a cybersecurity perspective," Online Journal of Communication and Media Technologies, vol. 14, no. 4, hlm. 1–15, Okt. 2024.

[17] N. Fisk et al., "Cybersecurity Communities of Practice: Strategies for Creating Gateways to Participation," ResearchGate, 2023.

[18] S. Nazir, "Impact of Machine Learning in Cybersecurity Augmentation," ResearchGate, 2023.

[19] T. Templin et al., "Privacy-Preserving Techniques in Generative AI and Large Language Models: A Narrative Review," MDPI, vol. 15, no. 11, 2024.

[20] G. Podgórski, "Analyzing Cyber-Attack Trends on an Educational Institution: A Case Study (2021–2023)," Eur. Res. Stud. J., vol. 27, no. S2, hlm. 444-453, Sep. 2024.

[21] R. C. Alexander, L. Ma, Z. Dou, Z. Cai, dan Y. Huang, "Integrity, Confidentiality, and Equity: Using Inquiry-Based Labs to help students understand AI and Cybersecurity," J. Cybersecurity Educ. Res. Pract., vol. 2024, no. 1, 2024.

[22] R. Pinto, R. Martins, dan C. Novo, "Infrastructure as Code for Cybersecurity Training," J. Cybersecurity Educ. Res. Pract., vol. 2024, no. 1, 2024.

[23] A. S. Al-Sherideh et al., "Assessing the Impact and Effectiveness of Cybersecurity Measures in e-Learning on Students and Educators: A Case Study," Int. J. Adv. Comput. Sci. Appl., vol. 14, no. 5, 2023.

[24] A. O. Dunmade, A. Tella, dan U. D. Onuoha, "A Developed Framework for Studying Cyberethical Behaviour in North Central Nigeria," J. Cybersecurity Educ. Res. Pract., vol. 2024, no. 1, 2024.

[25] R. Hamid, I. Fitrianto, dan A. Mulalic, "Exploring the Effectiveness of Hybrid Learning Models in Higher Education Post-Pandemic," Int. J. Post Axial, vol. 2, no. 3, hlm. 188-202, Sep. 2024.

[26] M. English dan J. Maguire, "The changing landscape in cybersecurity education, the impact of COVID-19, and the promise of online education programs," Issues Inf. Syst., vol. 24, no. 1, 2023.