p.mail

by ronisetyawan106@gmail.com 1

Submission date: 20-Aug-2025 08:37AM (UTC+0700)
Submission ID: 2732140399
File name: artikel_revisi_-_submit_Template_Jurnal_Empowerment_Aiska.docx (757.92K)
Word count: 3097
Character count: 21062

Volume 4 No.2 September 2024
E-ISSN : 2808-2478
Website : https://journal.aiska-university.ac.id/index.php/empowerment
E-mail : empowerment@aiska-university.ac.id
Doi : https://doi.org/10.30787/empowerment.v4i2.1458

EMPOWERMENT JOURNAL
Universitas 'Aisyiyah Surakarta
Universitas 'Aisyiyah Surakarta

PENINGKATAN KAPASITAS MAHASISWA DALAM BIDANG AI DAN KEAMANAN SIBER UNTUK MENCEGAH ANCAMAN DI DUNIA DIGITAL

Ismail setiawan[1], Ridho Surya Kusuma[2], Taqy Muhammad Fadhil[3], Ilma Nafisah Miftahul Jannah[4]
[1,3,4] Fakultas Sains Dan Teknologi Informasi, Universitas 'Aisyiyah Surakarta, Jawa Tengah, Indonesia
[2] Program StudiPJJInformatika, Universitas Siber Muhammadiyah, Yogyakarta, Indonesia
email: ismailsetiawan@aiska-university.ac.id

ABSTRAK

Kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan kapasitas mahasiswa di bidang kecerdasan buatan (AI) dan keamanan siber melalui pelatihan dan workshop yang dirancang berbasis Standar Kompetensi Kerja Nasional Indonesia (SKKNI) No. 55 Tahun 2015. Program ini menyasar mahasiswa Program Studi Sistem Informasi dan Teknologi Informasi dari mitra, yang masih memiliki keterbatasan dalam pengetahuan serta keterampilan praktis terkait ancaman digital. Metode pelaksanaan menggabungkan pelatihan langsung, pembelajaran berbasis proyek, dan e-learning mandiri. Hasil evaluasi menunjukkan peningkatan signifikan pada skor pre-test dan post-test peserta, penyelesaian proyek mini berbasis unit kompetensi, serta kepuasan tinggi terhadap pelaksanaan kegiatan. Selain dampak langsung, kegiatan ini juga mendorong terbentuknya komunitas belajar keamanan siber di kampus mitra dan peningkatan kesadaran digital peserta. Kendala teknis seperti keterbatasan perangkat dan pemahaman awal diatasi melalui pendekatan bertahap dan alternatif media pembelajaran. Program ini terbukti efektif dalam memperkuat kesiapan mahasiswa menghadapi tantangan keamanan digital dan berpotensi dikembangkan lebih lanjut secara berkelanjutan. Hasil evaluasi menunjukkan peningkatan signifikan pada skor pre-test dan post-test peserta, dengan rata-rata peningkatan nilai dari 58,75 menjadi 83,75 (naik sebesar 25 poin atau 42,55%), penyelesaian proyek mini berbasis unit kompetensi, serta kepuasan tinggi terhadap pelaksanaan kegiatan.

Kata Kunci: Artificial Intelligence; Cybersecurity; E-learning; Keamanan Informasi; Pelatihan Mahasiswa

ABSTRACT

This community service activity aims to enhance students' capacity in the fields of Artificial Intelligence (AI) and cybersecurity through training and workshops designed based on the Indonesian National Work Competency Standards (SKKNI) No. 55 of 2015. The program targets students of the Information Systems and Information Technology Study Program from the partner institution, who still lack knowledge and practical skills related to digital threats. The implementation method combines direct training, project-based learning, and self-paced e-learning. Evaluation results show a significant increase in participants' pre-test and post-test scores, completion of mini projects based on competency units, and high satisfaction with the activity. In addition to direct outcomes, the activity also encouraged the formation of a cybersecurity learning community at the partner campus and increased participants' digital awareness. Technical challenges, such as limited hardware and initial understanding, were addressed through a step-by-step teaching approach and alternative learning media. This program has proven effective in strengthening students' readiness to face digital security challenges and has the potential to be further developed sustainably.

***Keywords**: Artificial Intelligence; Cybersecurity; E-learning; Information Security; Student Training*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa transformasi signifikan dalam berbagai aspek kehidupan, termasuk dunia pendidikan tinggi (Dzaky & Edrisy, 2025; Gkioulos & Chowdhury, 2021). Di tengah derasnya arus digitalisasi, ancaman terhadap keamanan siber menjadi

isu yang semakin krusial. Serangan seperti phishing, malware, dan peretasan bukan lagi menjadi isu khusus kalangan professional tetapi telah menyasar masyarakat umum, termasuk mahasiswa (Afifah et al., 2025; Casino et al., 2023; Levy-Loboda et al., 2021; Mahendran & Velusamy, 2020; Prasetyo et al., 2024). Sayangnya, banyak mahasiswa di lingkungan perguruan tinggi, khususnya di program studi Sistem Informasi dan Teknologi Informasi, belum memiliki bekal pengetahuan dan keterampilan yang memadai untuk menghadapi tantangan ini. Kondisi ini diperparah dengan masih rendahnya pemanfaatan teknologi kecerdasan buatan (Artificial Intelligence/AI) dalam konteks praktis di kalangan mahasiswa (Hartanto et al., 2025; Patiño-Vanegas et al., 2023). Padahal, berbagai studi terkini menunjukkan bahwa integrasi AI dalam sistem keamanan informasi dapat meningkatkan efektivitas deteksi dan penanganan ancaman digital secara signifikan (Schiff, 2021). Bashir & Arora, (2023) menyoroti pentingnya pendekatan organisasi berbasis AI dalam merespons ancaman siber, sedangkan Blažič, (2021) mengembangkan model pembelajaran mendalam (deep learning) untuk sistem keamanan di sektor publik dan Pendidikan (Lakhno et al., 2022). Namun, inovasi seperti ini belum banyak dijadikan referensi dalam penguatan kapasitas mahasiswa secara langsung di ruang-ruang pelatihan atau kurikulum luar kelas (Rao & Elias-Medina, 2024).

Urgensi inilah yang melatarbelakangi penyusunan program pengabdian kepada masyarakat dalam bentuk pelatihan dan workshop bertema “Peningkatan Kapasitas Mahasiswa pada Bidang AI dan Keamanan Siber: Mencegah Ancaman di Dunia Digital”. Program ini diarahkan untuk menjawab tantangan aktual yang dihadapi mitra, yakni terbatasnya pengetahuan, keterampilan teknis, dan akses terhadap teknologi keamanan siber yang praktis dan aplikatif. Selain itu, terdapat kebutuhan yang kuat dari pihak mitra untuk meningkatkan literasi dan kesiapan mahasiswa terhadap tantangan dunia digital yang nyata. Rasionalisasi kegiatan ini juga sejalan dengan fokus kebijakan pendidikan tinggi dalam memperkuat kompetensi lulusan, mendorong pengalaman belajar di luar kelas, dan membangun kolaborasi antara institusi pendidikan dengan pihak eksternal. Kegiatan ini juga bersinergi dengan kebijakan kampus berdampak yang mendorong pembelajaran berbasis proyek, lintas disiplin, dan relevan dengan kebutuhan dunia kerja digital.

Mitra dalam program ini adalah Universitas Sibermu. Permasalahan utama yang dihadapi mitra meliputi rendahnya literasi keamanan siber di kalangan mahasiswa, keterbatasan pengalaman praktik menggunakan perangkat dan perangkat lunak keamanan informasi, serta belum terintegrasinya teknologi AI dalam kegiatan pembelajaran nonformal. Selain itu, akses mahasiswa terhadap sarana pendukung seperti laboratorium keamanan siber dan modul pembelajaran digital masih sangat terbatas. Hasil asesmen awal melalui pre-test terhadap empat mahasiswa mitra menunjukkan rata-rata skor sebesar 58,75 dari skala 100. Angka ini mengindikasikan bahwa tingkat pemahaman mahasiswa terkait konsep keamanan siber dan penerapan kecerdasan buatan masih tergolong rendah. Nilai tersebut berada di bawah standar minimal kompetensi dasar yang direkomendasikan oleh SKKNI No. 55 Tahun 2015, sehingga menunjukkan adanya kesenjangan kompetensi (competency gap) yang signifikan. Kondisi ini memperkuat kebutuhan akan intervensi pembelajaran yang terstruktur, aplikatif, dan selaras dengan standar kompetensi kerja nasional untuk memastikan mahasiswa siap menghadapi tantangan keamanan digital.

Solusi yang ditawarkan melalui program ini adalah penyelenggaraan pelatihan dan workshop berbasis Standar Kompetensi Kerja Nasional Indonesia (SKKNI) No. 55 Tahun 2015 dengan pendekatan blended learning, integrasi simulasi AI, dan pengembangan modul pembelajaran digital yang dapat diakses mandiri. Target capaian program ini meliputi peningkatan rata-rata nilai post-test minimal 20 poin dibanding pre-test, tersusunnya modul pelatihan berbasis SKKNI, terbentuknya komunitas belajar keamanan siber di kampus mitra, serta meningkatnya kesadaran dan keterampilan mahasiswa dalam mengidentifikasi dan mengantisipasi ancaman digital.

Dalam pelaksanaannya, program ini dirancang tidak hanya sebagai bentuk penyuluhan, tetapi juga mengadopsi pendekatan berbasis inovasi dan penguatan teknologi pembelajaran. Upaya ini mencakup pengembangan modul pembelajaran, pemanfaatan platform e-learning, serta penyusunan studi kasus praktis berbasis skenario nyata. Di samping itu, terdapat potensi kolaborasi lanjutan dari pihak mitra dan stakeholder lain seperti komunitas teknologi lokal atau lembaga pelatihan digital untuk memperluas dampak kegiatan ini di masa mendatang. Dengan demikian, kegiatan ini tidak hanya menjawab kebutuhan jangka pendek mahasiswa dan mitra, tetapi juga menjadi langkah awal menuju pembentukan ekosistem pembelajaran keamanan siber dan AI yang berkelanjutan, kontekstual, dan berorientasi pada penguatan kapasitas sumber daya manusia di era digital (Patiño-Vanegas et al., 2023).

METODE

Kegiatan pengabdian kepada masyarakat ini menggunakan metode kombinasi antara pelatihan langsung (*direct training*), pendekatan praktik berbasis proyek (*project-based learning*), dan pembelajaran daring mandiri (*self-paced e-learning*). Kombinasi ini dipilih untuk mengakomodasi kebutuhan mahasiswa dalam memahami konsep keamanan siber dan kecerdasan buatan secara komprehensif, sekaligus memungkinkan mereka mengembangkan keterampilan praktis yang relevan dengan konteks dunia digital. Pelaksanaan kegiatan dilakukan di ruang pertemuan Hotel Malioboro Inn, Yogyakarta, sebagai mitra pelaksanaan. Kegiatan berlangsung selama tiga hari, mulai 8–10 Juli 2025, yang mencakup tahap persiapan materi, pelatihan, workshop, serta evaluasi dan tindak lanjut pembelajaran mandiri melalui platform e-learning. Rangkaian kegiatan diawali dengan penyusunan modul pelatihan berbasis studi kasus dan skenario nyata mengenai keamanan siber serta penerapan AI. Selanjutnya, peserta mengikuti sesi pelatihan keamanan siber yang berisi materi dan praktik dasar tentang ancaman siber seperti *phishing*, *malware*, dan teknik mitigasi. Kegiatan dilanjutkan dengan workshop penerapan AI, di mana mahasiswa diperkenalkan pada dasar-dasar *machine learning* dan diarahkan untuk mengembangkan model sederhana untuk deteksi ancaman digital. Setelah itu, peserta mendapatkan akses ke modul digital dan platform e-learning untuk mendukung keberlanjutan pembelajaran secara mandiri. Tahap akhir berupa evaluasi dan monitoring dilakukan untuk menilai pemahaman peserta dan efektivitas metode melalui instrumen tes dan pengamatan.

Pengumpulan data dilakukan melalui beberapa cara. Pertama, pre-test dan post-test digunakan untuk mengukur peningkatan pengetahuan peserta. Kedua, kuesioner evaluasi kepuasan mengukur kualitas materi, fasilitator, dan fasilitas yang digunakan. Ketiga, monitoring platform e-learning dilakukan untuk melihat partisipasi dan tingkat penyelesaian modul pembelajaran. Keempat, penilaian proyek mini dilakukan untuk mengevaluasi kemampuan peserta dalam mengimplementasikan konsep yang telah dipelajari. Data yang terkumpul dianalisis secara kuantitatif dan kualitatif. Hasil pre-test dan post-test dianalisis menggunakan analisis komparatif sederhana untuk mengetahui peningkatan pengetahuan peserta. Data kepuasan peserta dan penyelesaian modul dianalisis secara deskriptif kuantitatif guna menggambarkan persepsi dan keterlibatan peserta. Sementara itu, analisis isi dilakukan terhadap proyek mini peserta untuk menilai sejauh mana pemahaman konsep dapat diimplementasikan secara mandiri.

HASIL PEMBAHASAN

Kegiatan pengabdian kepada masyarakat bertema *Peningkatan Kapasitas Mahasiswa pada Bidang AI dan Keamanan Siber* telah berhasil dilaksanakan dengan menggabungkan pendekatan

pelatihan langsung, pembelajaran berbasis proyek, dan modul digital berbasis e-learning. Fokus utama kegiatan ini adalah meningkatkan kompetensi mahasiswa dalam memahami konsep serta praktik dasar keamanan informasi dan kecerdasan buatan, dengan integrasi materi dari SKKNI (Standar Kerangka Kerja Nasional Indonesia) No. 55 Tahun 2015 bidang Keamanan Teknologi Informasi.

Seluruh rangkaian pelatihan dan workshop merujuk pada tujuh unit kompetensi dari SKKNI, yaitu menerapkan prinsip perlindungan informasi, menerapkan prinsip keamanan informasi untuk penggunaan jaringan internet, menerapkan prinsip keamanan informasi pada transaksi elektronik, melaksanakan kebijakan keamanan informasi, mengaplikasikan ketentuan atau persyaratan keamanan informasi, mengelola log, dan menerapkan kontrol akses berdasarkan konsep atau metodologi yang telah ditetapkan. Penyampaian unit-unit ini dilakukan melalui simulasi kasus, diskusi interaktif, dan latihan praktik menggunakan perangkat lunak keamanan jaringan serta platform AI sederhana. Pelaksanaan kegiatan menghasilkan sejumlah luaran langsung yang signifikan. Sebanyak empat orang peserta, yang merupakan mahasiswa Program Studi Sistem Informasi dan Teknologi Informasi, berhasil menyelesaikan seluruh rangkaian pelatihan dengan partisipasi penuh. Dua kegiatan utama yang dilaksanakan adalah pelatihan keamanan siber dan workshop penerapan AI, yang masing-masing dirancang untuk memperkuat aspek teknis dan analitis peserta sesuai dengan unit kompetensi SKKNI. Sebagai penunjang keberlanjutan, tim pelaksana menyusun modul pelatihan digital berbasis SKKNI dan mengintegrasikan teknologi AI ke dalam skenario pembelajaran, baik dalam bentuk materi ajar maupun simulasi penggunaan *tools* seperti Wireshark dan RapidMiner. Modul ini dikembangkan untuk mendukung model e-learning dan dapat diakses secara mandiri oleh peserta setelah pelatihan.

Hasil evaluasi pembelajaran melalui pre-test dan post-test menunjukkan peningkatan nilai yang signifikan pada seluruh peserta, dengan rata-rata kenaikan sebesar 25 poin, yang mencerminkan peningkatan pemahaman nyata terhadap materi keamanan informasi dan AI. Seluruh peserta mampu menyelesaikan proyek mini yang disesuaikan dengan tujuh unit kompetensi, seperti pengelolaan log, kontrol akses, dan perlindungan data dalam transaksi elektronik. Tingkat penyelesaian modul e-learning juga tinggi, dengan capaian antara 90–100%. Hal ini menunjukkan efektivitas pendekatan *blended learning* yang digunakan, serta mengindikasikan motivasi dan kemampuan peserta untuk mengikuti instruksi teknis secara mandiri.

Selain luaran langsung, kegiatan ini juga memberikan dampak tidak langsung yang bersifat kualitatif dan berkelanjutan. Peserta menunjukkan peningkatan kesadaran akan pentingnya perlindungan informasi, tidak hanya dari sisi teknis, tetapi juga dalam dimensi sosial dan profesional. Mereka menjadi lebih berhati-hati dalam mengelola informasi pribadi dan institusional, serta memiliki kesadaran etis terkait penggunaan jaringan internet dan keamanan dalam transaksi digital. Kegiatan ini juga memicu terbentuknya komunitas belajar keamanan siber di lingkungan kampus, yang menjadi wadah berbagi pengetahuan, diskusi topik terkini, dan perencanaan kegiatan lanjutan seperti pelatihan atau proyek kolaboratif.

Dari sisi keunggulan, strategi pelaksanaan yang digunakan terbukti efektif dalam meningkatkan kualitas pembelajaran dan kepuasan peserta. Integrasi materi berbasis SKKNI memberikan kerangka belajar yang terstandarisasi dan terstruktur, membantu peserta memahami keterkaitan antara teori dan praktik secara sistematis. Penggunaan simulasi dan proyek mini meningkatkan keterlibatan aktif, memacu kemampuan memecahkan masalah nyata, dan membangun kepercayaan diri peserta dalam menghadapi tantangan profesional. Pendekatan *blended learning* juga memberi fleksibilitas bagi peserta untuk mengakses materi, mengulang simulasi, dan berdiskusi secara daring. Evaluasi kepuasan menunjukkan rata-rata skor di atas 4 dari skala 5, menandakan bahwa desain kegiatan sesuai dengan kebutuhan peserta dan memberikan pengalaman belajar yang bermakna. Meskipun berjalan lancar, beberapa tantangan dihadapi selama pelaksanaan. Terbatasnya waktu pelatihan menjadi kendala karena materi yang disampaikan cukup padat dan teknis, sesuai dengan unit-unit kompetensi SKKNI.

Keterbatasan perangkat keras dan perangkat lunak juga mempengaruhi kelancaran simulasi AI dan keamanan jaringan. Beberapa peserta kesulitan menjalankan aplikasi tertentu karena spesifikasi perangkat yang rendah, sehingga tim menyediakan alternatif berupa simulasi video dan akses terbatas ke *lab* virtual. Selain itu, rendahnya pemahaman awal tentang AI dan log keamanan menyebabkan sebagian peserta kesulitan di awal pelatihan. Untuk mengatasinya, metode pengajaran disesuaikan secara bertahap dengan pemberian materi pengantar yang lebih kontekstual. Kendala-kendala ini menjadi bahan evaluasi penting untuk perbaikan di pelatihan berikutnya, khususnya dalam aspek teknis, durasi, dan kesiapan perangkat.

Tabel 1. Unit Kompetensi SKKNI No. 55 Tahun 2015 – Bidang Keamanan Teknologi Informasi

No.	Kode Unit	Judul Unit
1	J.62090.001.01	Menerapkan Prinsip Perlindungan Informasi
2	J.62090.003.01	Menerapkan Prinsip Keamanan Informasi untuk Penggunaan Jaringan Internet
3	J.62090.004.01	Menerapkan Prinsip Keamanan Informasi pada Transaksi Elektronik
4	J.62090.006.01	Melaksanakan Kebijakan Keamanan Informasi
5	J.62090.012.01	Mengaplikasikan Ketentuan/Persyaratan Keamanan Informasi
6	J.62090.020.01	Mengelola Log
7	J.62090.032.01	Menerapkan Kontrol Akses Berdasarkan Konsep/Metodologi yang Telah Ditetapkan

Gambar 1. Pelatihan Junior Cyber Security

Tabel 2. Jadwal Pelatihan / Workshop

No	Kegiatan	Tanggal	Waktu
1	Pelatihan Keamanan Siber	5 Mei 2025	09.00–12.00
2	Workshop Penerapan AI	6 Mei 2025	13.00–16.00

Tabel 3. Pre-Test dan Post-Test

No	Nama Peserta	Pre-Test	Post-Test	Selisih	Keterangan
1	Mahasiswa 1	60	85	+25	Naik
2	Mahasiswa 2	58	82	+24	Naik
3	Mahasiswa 3	62	88	+26	Naik
4	Mahasiswa 4	55	80	+25	Naik

Tabel 4. Monitoring Platform E-Learning

No	Nama Peserta	Total Modul	Modul Selesai	Persentase	Terakhir Akses
1	Mahasiswa 1	10	10	100%	28 Mei 2025
2	Mahasiswa 2	10	9	90%	27 Mei 2025
3	Mahasiswa 3	10	10	100%	28 Mei 2025
4	Mahasiswa 4	10	8	80%	26 Mei 2025

Tabel 5. Penilaian Tugas Praktik / Proyek Mini

No	Nama Peserta	Judul Proyek Mini	Skor	Keterangan
1	Mahasiswa 1	Deteksi Email Phishing dengan AI	88	Lulus
2	Mahasiswa 2	Analisis Serangan Brute Force	82	Lulus
3	Mahasiswa 3	AI untuk Deteksi Ransomware	90	Lulus
4	Mahasiswa 4	Proteksi Jaringan Mahasiswa	80	Lulus

Tabel 6. Distribusi Modul Pelatihan

No	Nama Peserta	Modul AI	Modul Keamanan Siber	Catatan
1	Mahasiswa 1	✓	✓	Lengkap
2	Mahasiswa 2	✓	✓	Lengkap
3	Mahasiswa 3	✓	✓	Lengkap
4	Mahasiswa 4	✓	✓	Lengkap

Tabel 7. Rekapitulasi Kegiatan

No	Nama Kegiatan	Tanggal	Lokasi	Jumlah Peserta	Dokumentasi
1	Pelatihan Keamanan Siber	5 Mei 2025	Aula FTI	4	Foto/Video
2	Workshop Penerapan AI	6 Mei 2025	Lab Komputer 1	4	Foto/Video

Tabel 8. Evaluasi Kepuasan Peserta

No	Nama Peserta	Fasilitas (1–5)	Materi (1–5)	Narasumber (1–5)	Saran
1	Mahasiswa 1	5	5	5	Sangat aplikatif, lanjutkan tiap tahun.
2	Mahasiswa 2	4	4	4	Tambahkan studi kasus nyata di tiap sesi.
3	Mahasiswa 3	5	5	5	Sediakan sertifikat elektronik juga.
4	Mahasiswa 4	4	4	5	Perbanyak sesi praktik hands-on.

Kegiatan ini menunjukkan bahwa penggabungan kerangka SKKNI dengan pendekatan praktikal dan digital dapat memperkuat pemahaman dan keterampilan mahasiswa di bidang keamanan informasi. Hal ini sejalan dengan temuan (Song & Luo, 2023) yang menyatakan bahwa keterampilan teknis keamanan informasi dapat ditingkatkan melalui pelatihan berbasis standar kompetensi dan simulasi. Selain itu, integrasi AI sebagai alat bantu deteksi ancaman siber mencerminkan penerapan teknologi mutakhir yang sejalan dengan arah industri 4.0 dan kebutuhan keamanan digital masa kini.

KESIMPULAN DAN SARAN

Secara keseluruhan, kegiatan pelatihan dan workshop yang berfokus pada keamanan siber dan kecerdasan buatan (AI) telah berhasil meningkatkan pengetahuan, keterampilan, serta kesadaran mahasiswa dalam menghadapi tantangan dunia digital. Pendekatan berbasis standar kompetensi, blended learning, serta penggunaan teknologi mutakhir terbukti efektif dalam meningkatkan partisipasi dan kepuasan peserta, meskipun terdapat kendala seperti keterbatasan perangkat dan pemahaman awal yang masih perlu ditingkatkan. Untuk keberlanjutan dan keberhasilan program di masa depan, disarankan agar fasilitas perangkat keras dan perangkat lunak diperkuat, materi pelatihan disusun secara kontekstual dan inovatif, serta modul digital dan platform e-learning terus diperbarui sesuai perkembangan teknologi. Selain itu, kolaborasi dengan komunitas teknologi dan lembaga lain serta evaluasi berkelanjutan juga penting dilakukan guna memperluas dampak dan memastikan peningkatan kapasitas mahasiswa yang berkelanjutan dalam bidang keamanan siber dan AI.

DAFTAR PUSTAKA

Afifah, E. F. N., Simatangkir, D. W. E., & Faliha, N. S. (2025). Keamanan Siber Dalam Perbankan Serta Tantangan Dan Solusi Di Era Digital. *Jurnal Multidisiplin Ilmu Akademik*, *2*(1), 33–42.

Bashir, S., & Arora, B. (2023). Prediction of Need for Cyber Training for University Students Using Artificial Neural Networks. *Procedia Computer Science*, *218*, 1414–1423. https://doi.org/https://doi.org/10.1016/j.procs.2023.01.120

Blažič, B. J. (2021). The cybersecurity labour shortage in Europe: Moving to a new concept for education and training. *Technology in Society*, *67*, 101769. https://doi.org/https://doi.org/10.1016/j.techsoc.2021.101769

Casino, F., Totosis, N., Apostolopoulos, T., Lykousas, N., & Patsakis, C. (2023). Analysis and Correlation of Visual Evidence in Campaigns of Malicious Office Documents. *Digital Threats: Research and Practice*, *4*(2), 1–19. https://doi.org/10.1145/3513025

Dzaky, M. A. T., & Edrisy, I. F. (2025). Strategi Pencegahan Kejahatan Siber di Indonesia: Sinergi antara UU ITE dan Kebijakan Keamanan Digital. *PESHUM: Jurnal Pendidikan, Sosial Dan Humaniora*, *4*(2), 3614–3625.

Gkioulos, V., & Chowdhury, N. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, *40*, 100361. https://doi.org/10.1016/j.cosrev.2021.100361

Hartanto, M. B., Winarko, T., Yunita, H. D., Fahurian, F., Yuniarthe, Y., & Zuhri, K. (2025). Model Prediksi Keamanan Siber Menggunakan Artificial Intelligence untuk Mitigasi Ancaman Digital:-. *Prosiding Seminar Nasional KONSTELASI*, *2*(1), 55–63.

Lakhno, V., Kydyralina, L., Akhmetov, B., Yagaliyeva, B., & Makulov, K. (2022). Analysis of Information Flows of Distance Education Systems, Taking into Account the Need to Ensure Their Cybersecurity. In *CEUR Workshop Proceedings* (Vol. 3288, pp. 104–109).

Levy-Loboda, T., Rav-Acha, M., Katz, A., & Nissim, N. (2021). Cardio-ML: Detection of malicious clinical programmings aimed at cardiac implantable electronic devices based on

machine learning and a missing values resemblance framework. *Artificial Intelligence in Medicine*, *122*, 102200. https://doi.org/https://doi.org/10.1016/j.artmed.2021.102200

Mahendran, R. K., & Velusamy, P. (2020). A secure fuzzy extractor based biometric key authentication scheme for body sensor network in Internet of Medical Things. *Computer Communications*, *153*, 545–552. https://doi.org/https://doi.org/10.1016/j.comcom.2020.01.077

Patiño-Vanegas, J. C., Mardones-Espinosa, R., Garcés-Giraldo, L. F., Valencia-Arias, A., Arango-Botero, D. M., & García, R. B. (2023). Research trends regarding the use of Artificial Intelligence in university contexts. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *2023*(E59), 245–260.

Prasetyo, H., Ibrahim, I., Moelyana, M. M. H., & Abid, Z. M. (2024). Keamanan Cyber dalam Menghadapi Tantangan Ancaman Masa Depan di Universitas Bhayangkara Jakarta Raya. *Journal of Informatic and Information Security*, *5*(2), 235–244.

Rao, A. R., & Elias-Medina, A. (2024). Designing an internet of things laboratory to improve student understanding of secure IoT systems. *Internet of Things and Cyber-Physical Systems*, *4*, 154–166. https://doi.org/https://doi.org/10.1016/j.iotcps.2023.10.002

Schiff, D. (2021). Out of the laboratory and into the classroom: the future of artificial intelligence in education. *AI and Society*, *36*(1), 331–348. https://doi.org/10.1007/s00146-020-01033-8

Song, Q., & Luo, W. (2023). SFBKT: A Synthetically Forgetting Behavior Method for Knowledge Tracing. *Applied Sciences (Switzerland)*, *13*(13), 7704. https://doi.org/10.3390/app13137704

p.mail

ORIGINALITY REPORT

17%	17%	7%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	journal.aiska-university.ac.id Internet Source	6%
2	bpptik.kominfo.go.id Internet Source	3%
3	adoc.tips Internet Source	2%
4	www.rctiplus.com Internet Source	1%
5	jipp.unram.ac.id Internet Source	1%
6	Submitted to Universitas Bengkulu Student Paper	<1%
7	journal.irpi.or.id Internet Source	<1%
8	Submitted to Universitas Tidar Student Paper	<1%
9	inspirasi.bpsdm.jabarprov.go.id Internet Source	<1%
10	jurnal-adaikepri.or.id Internet Source	<1%
11	jurnal.syntax-idea.co.id Internet Source	<1%
12	jurnal.umpwr.ac.id Internet Source	<1%

13	e-journal.trisakti.ac.id Internet Source	<1 %
14	journal.diginus.id Internet Source	<1 %
15	melanchthon.nl Internet Source	<1 %
16	new.jurnal.untad.ac.id Internet Source	<1 %
17	repository.uib.ac.id Internet Source	<1 %
18	Endah Heryanti, Hendra Kasman, Wetri Efita, Olivia Tahalele, Asmawati Asmawati, Conny Oktizulvia. "PELATIHAN PENGGUNAAN ARTIFICIAL INTELLIGENCE (AI) DALAM DESAIN PEMBELAJARAN INOVATIF BAGI DOSEN", Community Development Journal : Jurnal Pengabdian Masyarakat, 2025 Publication	<1 %
19	bnsp.go.id Internet Source	<1 %
20	fst.aiska-university.ac.id Internet Source	<1 %
21	lume.ufrgs.br Internet Source	<1 %
22	sib.stts.edu Internet Source	<1 %
23	www.scribd.com Internet Source	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		