PROSIDING Seminar Nasional SISFOTEK ISSN 2597-3584 (Media Online)
Sistem Informasi dan Teknologi
website : www.seminar.iaii.or.id | email : seminar@iaii.or.id

Mapping Review Penerapan Artificial Intelligence pada Cyber Security untuk Meningkatkan Security Awareness

I Putu Agus Eka Pratama[1*], I Made Oka Widyantara[2], Linawati[2], Nyoman Gunantara[2]
[1]Program Studi Doktor Ilmu Teknik, Fakultas Teknik, Universitas Udayana
[2]Program Studi Teknik Elektro, Fakultas Teknik, Universitas Udayana
eka.pratama@unud.ac.id

Abstract

The rapid development of information technology (IT), on the one hand, has the potential to increase the number of cyber attacks, so cyber security needs to be handled properly. As the weakest element, efforts are needed to increase cyber security awareness on the user side. Artificial intelligence (AI), which is increasingly developing and widely applied in various fields of life, has the potential to be used to increase security awareness in users. To study this further, a literature study, review, and mapping analysis were conducted from a number of references in order to obtain an overview of the potential and future research plans related to the use of AI in cyber security for security awareness along with providing recommendations. This study conducted a study and analysis using the mapping review method on 37 selected papers indexed by Google Scholar, referring to the NIST (National Institute of Standards and Technology) framework. The results of the mapping review show that the mapping of publications related to the application of AI to cyber security to increase security awareness is the most in 2024, with the most trends being education/training, and the most widely used AI method is deep learning. This study recommends education and deep learning as areas that can be taken for future research related to the application of AI to cyber security.

Keywords: Artificial intelligence (AI), cyber security, mapping review, NIST, security awareness.

Abstrak

Perkembangan Teknologi Informasi (TI) yang makin pesat, di satu sisi menimbulkan potensi peningkatan jumlah serangan siber, sehingga keamanan siber (cyber security) perlu untuk ditangani dengan baik. Sebagai elemen terlemah, diperlukan upaya untuk meningkatkan kesadaran keamanan siber (security awareness) di sisi pengguna. Artificial Intelligence (AI) yang semakin berkembang dan banyak diterapkan pada berbagai bidang kehidupan, memiliki potensi untuk dapat digunakan di dalam meningkatkan security awareness pada pengguna. Untuk mengkaji hal ini lebih lanjut, dilakukan studi literatur, tinjauan, dan analisis pemetaan dari sejumlah referensi, agar dapat memperoleh gambaran potensi dan rencana penelitian ke depannya terkait pemanfaatan AI pada cyber security untuk security awarenes beserta pemberian rekomendasi. Penelitian ini melakukan kajian dan analisis menggunakan metode mapping review terhadap 37 paper terseleksi yang terindeks Google Scholar, dengan mengacu kepada framework NIST (National Institute of Standards and Technology). Hasil mapping review menunjukkan bahwa pemetaan publikasi terkait penerapan AI pada cyber security untuk meningkatkan security awareness terbanyak di tahun 2024, dengan tren terbanyak berupa edukasi/pelatihan/training, dan metode AI yang paling banyak digunakan adalah Deep Learning. Penelitian ini merekomendasikan edukasi dan Deep Learning sebagai bidang yang dapat diambil untuk penelitian ke depannya terkait penerapan AI pada cyber security.

Kata kunci: Artificial Intelligence (AI), cyber security, mapping review, NIST, security awareness.

1. Pendahuluan

Teknologi Informasi (TI) yang makin berkembang pesat, sangat membantu manusia di segala bidang kehidupan. Namun di sisi lain, hal ini turut meningkatkan jumlah kasus serangan siber. Lanskap keamanan siber Indonesia tahun 2023 dari BSSN menunjukkan bahwa Indonesia merupakan 10 besar negara dengan sumber serangan siber dan tujuan serangan siber tertinggi di dunia, di mana target tertinggi adalah pengguna [1]. Hal ini disebabkan oleh karena di dalam elemen keamanan siber, pengguna merupakan elemen terlemah [2], sehingga memicu bentuk-bentuk serangan siber berupa social engineering, ransomware, malware, phising, hingga Advanced Persistent Threat (APT) yang memanfaatkan kelemahan di sisi manusia [3].

Untuk menanggulangi permasalahan ini, diperlukan upaya peningkatan kesadaran keamanan siber (security awareness). Security awareness merupakan pengetahuan, pemahaman, dan sikap dari pengguna komputer (individu, organisasi) mengenai cyber security yang mencakup perlindungan aset fisik, data, informasi, serta privasi individu dan organisasi [4]. Security awareness dibedakan menjadi tiga domain

yaitu kesadaran keamanan informasi (Information Security Awareness), kesadaran keamanan di ranah siber (Cyber Security Awareness), dan kesadaran keamanan di sisi pengguna (User Security Awareness).

Sejumlah solusi telah tersedia untuk membantu meningkatkan security awareness, antara lain: a.)Penyediaan sumber referensi panduan keamanan siber secara gratis di internet, b.)Penyediaan pelatihan keamanan siber, c.)Layanan konsultasi siber berbayar melalui jasa konsultan. Namun layanan-layanan ini belum mampu sepenuhnya meningkatkan security awareness.

Perkembangan TI yang makin pesat, semestinya dapat membantu memberikan solusi atas permasalahan ini. Salah satu TI yang berkembang pesat dan cukup banyak dipakai saat ini adalah Artificial Intelligence (AI). Artificial Intelligence (AI) didefinisikan sebagai sub bidang keilmuan komputer dan perangkat lunak komputer (software) yang bertujuan untuk memecahkan permasalahan sehari-hari yang bersifat kognitif, yang berkaitan dengan upaya meniru kecerdasan makhluk hidup (manusia, hewan, tumbuhan) sebagai sebuah kecerdasan buatan, ke dalam bentuk software untuk dapat melakukan penciptaan, pengenalan gambar, prediksi, serta pembelajaran pada mesin komputer berbasiskan data latih dan dataset[5].

Terkait dengan penelitian ini, di mana AI diterapkan pada ranah cyber security, maka secara spesifik AI merupakan software yang dikhususkan untuk dapat memecahkan permasalahan terkait cyber security, yang mampu menganalisis permasalahan siber di lingkungan jaringan dan sistem sekaligus memberikan solusi, penanganan, dan tindakan, dengan mengadopsi kecerdasan makhluk hidup [6]. Dengan demikian, AI memiliki kemampuan meniru cara kerja dari manusia, hewan, tumbuhan, dan bentuk makhluk hidup lainnya di dalam bertahan terhadap serangan siber sekaligus melakukan respon terkait serangan siber.

Namun untuk dapat memahami penerapan AI pada ranah *cyber security* di dalam upaya meningkatkan security awareness, perlu dilakukan kajian lebih lanjut melalui studi literatur, tinjauan, dan analisis pemetaan dari sejumlah referensi paper. Hal ini bertujuan untuk dapat memperoleh gambaran mengenai bentuk-bentuk penerapan AI pada ranah *cyber security* untuk meningkatkan security awareness. Kajian perlu dilakukan untuk referensi kurun waktu minimal satu dekade, untuk dapat memhami tren perkembangan di bidang dan topik ini.

Untuk mendukung kajian dan pemetaan penerapan AI pada *cyber security* untuk meningkatkan security awareness, diperlukan acuan sebuah *framework* di bidang *cyber security*. Framework NIST yang dikembangkan oleh National Institute of Standards and Technology [7], dipilih menjadi acuan didalam penelitian ini. Framework NIST terdiri atas lima elemen dengan perincian sebagai berikut:

Identify, di mana elemen ini meliputi: asset management, business environment, governance, risk assessment, risk management strategy, supply chain risk management.

Protect, di mana elemen ini meliputi: identity management and access control, awareness and training, data security, information protection process and procedure, protective technology.

Detect, di mana elemen ini meliputi: anomalies and events, security continous monitoring, detection process.

Respond, di mana elemen ini meliputi: response planning, communication, analysis, mitigation, improvement.

Recover, di mana elemen ini meliputi: recovery planning, improvement, communication.

Mengacu kepada kelima elemen Framework NIST, fokus di dalam penelitian ini adalah pada elemen Protect, khususnya pada Awareness and Training. Untuk metode kajian analisis dan pemetaan digunakan metode Mapping Review.

Rumusan masalah penelitian ini yaitu bagaimana pemetaan penerapan AI pada ranah cyber security untuk meningkatkan security awareness dalam kurun waktu satu dekade (2014-2024) beserta potensi ke depannya, berbasiskan kepada framework NIST khususnya pada elemen Protect berupa Awareness and Training. Tujuan penelitian ini yaitu memperoleh gambaran mengenai pemetaan penerapan AI pada *cyber security* untuk meningkatkan security awarensss dalam kurun waktu satu dekade (2014-2024) dari sisi metode, tren, potensi, untuk kemudian dilakukan pemberian rekomendasi.

2. Metode Penelitian

Mapping review merupakan metode ilmiah untuk memetakan suatu bidang atau topik penelitian, agar dapat menentukan area-area yang berpotensi untuk diteliti lebih lanjut, menentukan posisi penelitian, memberikan kerangka kerja dan gambaran penelitian empiris secara lebih jelas, serta membantu pemberian rekomendasi untuk langkah penelitian ke depannya[8]. Mapping review dapat dilakukan terhadap berbagai bidang ilmu dengan memanfaatkan sejumlah referensi paper ilmiah dalam kurun waktu tertentu, untuk dapat mengetahui trend dari topik keilmuan tersebut[9]. Dengan demikian, mapping review dapat menggunakan paper-paper publikasi ilmiah dari berbagai jurnal dan proceeding dengan berbagai indexing (Google Scholar, Scopus, WoS) dan mendukung penelitian kualitatif maupun kuantitatif secara sistematis[10].

Terdapat lima langkah di dalam metode mapping review, yaitu: 1.)Menentukan pertanyaan penelitian (Research Question/RQ), 2.)Memilih sumber referensi dan indexing yang tepat, 3.)Memilih kata kunci

pencarian (keyword) yang tepat, 4.)Seleksi hasil pencarian untuk memperoleh hasil relevan, 5.)E kstraksi dan sintesis data[10]. Kelima langkah ini perlu dilakukan secara terurut untuk dapat memberikan hasil yang baik.

Pertanyaan penelitian (Research Question atau RQ) disusun untuk memperkuat rumusan masalah pada penelitian ini, sekaligus menjadi acuan mapping review dari sisi jawaban yang diperoleh. Terdapat tiga pertanyaan penelitian (RQ) pada penelitian ini, yaitu:

RQ1:Bagaimana pemetaan publikasi terkait pemanfaatan AI pada cyber security untuk meningkatkan security awareness?

RQ2: Bagaimana trend penerapan AI pada cyber security untuk meningkatkan security awareness pada kurun waktu satu dekade (2014-2024)?

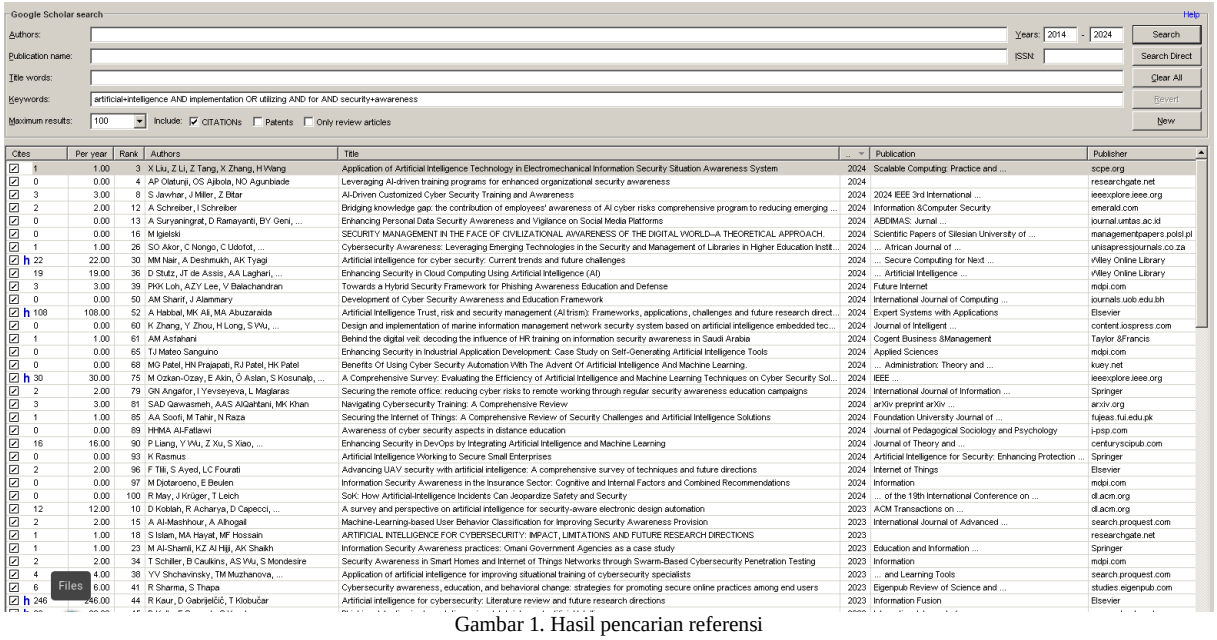
RQ3: Apa saja metode AI yang diterapkan pada cyber security untuk mendukung security awareness?

Pemilihan sumber-sumber referensi yang akan dikaji menggunakan mapping review pada penelitian ini, dilakukan menggunakan software Publish or Perish (PoP) pada sistem operasi Linux Ubuntu. PoP menyajikan hasil pencarian berupa paper publikasi pada jurnal ilmiah dan proceeding sesuai indexing yang dipilih. Pada penelitian ini digunakan sumber referensi paper pada jurnal dan proceeding yang terindeks Google Scholar, dengan pertimbangan bahwa semua paper publikasi cenderung akan terindex pada Google Scholar (selain juga pada indexing lainnya) dan bersifat umum, sehingga memperbesar kemungkinan untuk memperoleh hasil pencarian yang lebih banyak.

Pemilihan kata kunci pencarian dilakukan dengan penyesuaian terhadap topik yang dikaji. Di dalam penelitian ini, topik yang dikaji adalah mengenai penerapan AI pada cyber security untuk meningkatkan security awareness. Kata kunci yang digunakan berupa query berikut:

artificial+intelligence AND implementation OR utilizing AND for AND security+awareness

Berdasarkan kepada query kata kunci yang digunakan, diperoleh 100 paper. Gambar 1. menunjukkan hasil dari PoP menggunakan kata kunci pencarian dengan sumber dari jurnal dan proceeding terindeks Google Scholar:



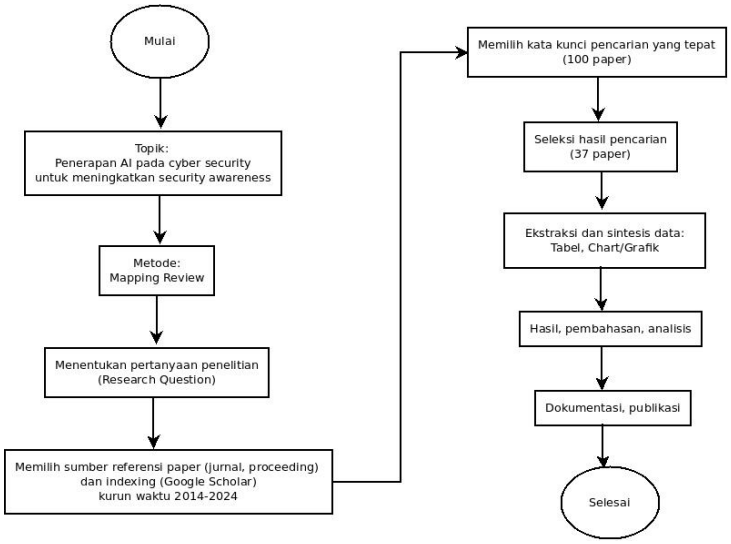
Gambar 1. Hasil pencarian referensi

Dari 100 paper yang telah diperoleh, kemudian dicek dan diseleksi lebih lanjut untuk mengetahui apakah terdapat paper yang tidak relevan dengan topik dan konteks penelitian. Untuk itu, dilakukan teknik inklusi dan eksklusi. Kriteria untuk inklusi meliputi: 1.)Paper terindeks minimal pada Google Scholar, 2.)Rentang tahun publikasi adalah 2014-2024, 3.)Bahasan pada paper berkaitan dengan AI, cyber security, dan security awareness.

Untuk kriteria eksklusi meliputi: 1.)Tidak termasuk paper (laporan penelitian, buku, paten, artikel web) dan tidak terindeks minimal pada Google Scholar, 2.)Rentang tahun publikasi sebelum 2014, 3.)Pembahasan tidak berkaitan dengan AI, cyber security, dan security awareness. Dari hasil seleksi, diperoleh 37 paper yang relevan.

Paper-paper yang relevan kemudian diolah melalui proses ekstraksi data dan sintesis data. Penulis menggunakan Libre Office Calc pada sistem operasi Linux Ubuntu untuk mencatat data-data paper yang akan diekstraksi dan disintesis berdasarkan kepada tahun publikasi dan pembahasan paper (tren penerapan AI, metode AI yang digunakan). Data-data pada tabel disajikan pada paper ini beserta dengan chart.

Flowchart penelitian menampilkan alur langkah yang ditampilkan pada Gambar 2.: dilakukan di dalam penelitian. Flowchart penelitian



Gambar 2. Flowchart penelitian

3. Hasil dan Pembahasan

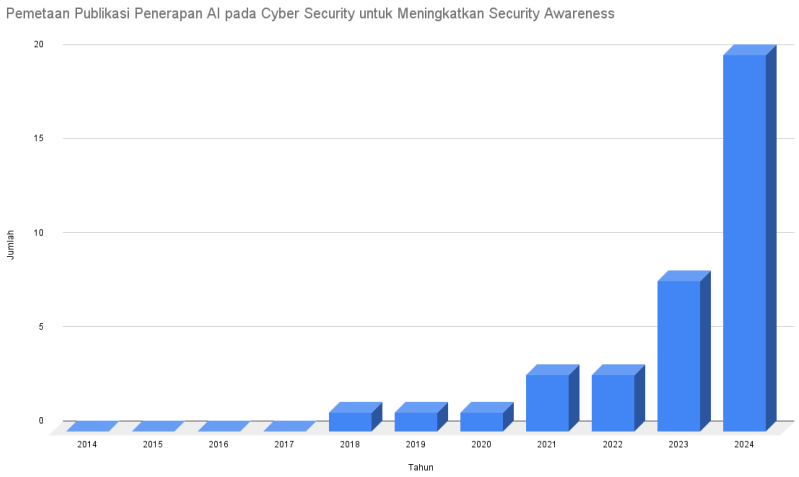
3.1. Pemetaan Publikasi

Untuk mengetahui pemetaan publikasi terkait pemanfaatan AI pada cyber security untuk meningkatkan security awareness, dilakukan pendataan terhadap 37 paper. Hasil pemetaan ditampilkan pada Tabel 1. dan grafik ditampilkan dalam bentuk chart pada Gambar 3.

Berdasarkan Tabel 1. dan Gambar 3., publikasi terbanyak mengenai penerapan AI pada cyber security untuk meningkatkan security awareness adalah pada tahun 2024. Sedangkan publikasi paling sedikit adalah di tahun 2018, 2019, dan 2020. Sementara itu, tidak ada publikasi pada tahun 2014 hingga 2017.

Tabel 1.Pemetaan Publikasi Penerapan AI pada Cyber Security untuk Meningkatkan Security Awareness

Tahun	Paper	Jumlah	Persentase
2014	-	0	0%
2015	-	0	0%
2016	-	0	0%
2017	-	0	0%
2018	[47]	1	2,7%
2019	[46]	1	2,7%
2020	[45]	1	2,7%
2021	[42],[43],[44]	3	8,1%
2022	[39],[40],[41]	3	8,1%
2023	[23],[27],[33],[34],[35],[36],[37],[38]	8	21,6%
2024	[11],[12],[13],[14],[15],[16],[17],[18],[19],[20],[21],[22],[24],[25],[26],[28],[29],[30],[31],[32]	20	54,1%



Gambar 3. Chart pemetaan publikasi penerapan AI pada cyber security untuk meningkatkan security awareness

Hal ini menunjukkan bahwa topik mengenai penerapan AI pada ranah cyber security untuk meningkatkan security awareness mulai muncul dan diminati oleh para peneliti per tahun 2018 dan mengalami

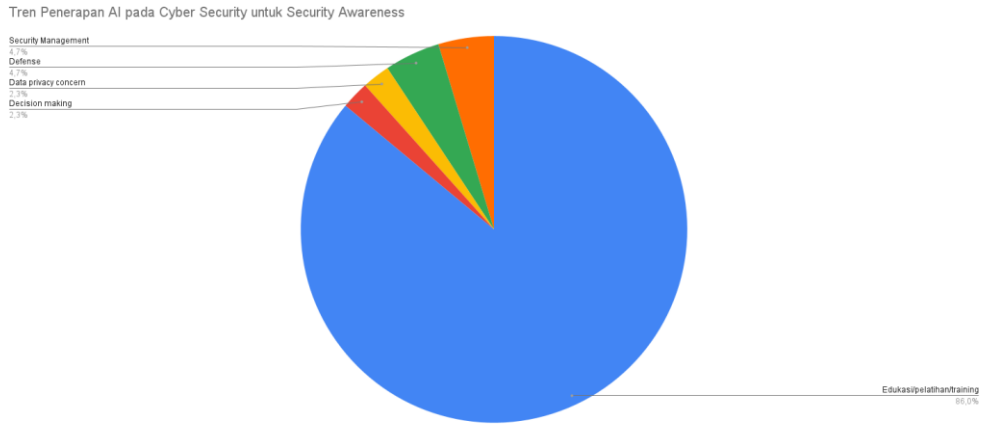
perkembangan pesat pada tahun 2023 dan 2024. Dengan demikian, sangat besar kemungkinan di tahun-tahun ke depannya, publikasi terkait topik ini akn terus bertambah seiring dengan makin banyaknya metode dan studi kasus yang dapat diangkat ke dalam paper penelitian.

3.2. Tren Penerapan AI Pada Cyber Security

Untuk mengetahui tren penerapan AI pada cyber security untuk meningkatkan security awareness, dilakukan pendataan terhadap 37 paper. Hasil pemetaan ditampilkan pada Tabel 2. dan grafik ditampilkan dalam bentuk chart pada Gambar 4.:

Tabel 2. Tren Penerapan AI pada Cyber Security untuk Security Awareness

Tren Penerapan AI pada Cyber Security	Paper	Jumlah
Edukasi/pelatihan/training	[11],[12],[13],[14],[15],[16],[17],[18],[19],[20],[21],[22],[23],[24],[25],[26],[27],[28],[29],[30],[31],[32],[33],[34],[35],[36],[37],[38],[39],[40],[41],[42],[43],[44],[45],[46],[47]	37
Decision making	[16]	1
Data privacy concern	[17]	1
Defense	[18],[36]	2
Security Management	[16],[20]	2



Gambar 4. Chart tren penerapan AI pada cyber security untuk security awareness

Berdasarkan Tabel 2. dan Gambar 4., tren penerapan AI pada cyber security untuk security awareness terbanyak berupa edukasi/pelatihan/training. Keseluruhan (37 paper) mengikuti tren ini, sedangkan beberapa lainnya juga mengambil tren security management (2 paper), defense (2 paper), data privacy concern (1 paper), dan decision making (1 paper).

Hal ini menunjukkan bahwa topik mengenai penerapan AI pada ranah cyber security untuk meningkatkan security awareness paling berpotensi untuk membantu di sisi edukasi/pelatihan/training. Berdasarkan hal ini, sangat berpotensi untuk ke depannya melakukan penelitian terkait dengan pengembangan metode, platform, prototipe, software, dan framework berbasis AI yang mendukung proses edukasi/pelatihan/training di bidang cyber security, khususnya untuk meningkatkan security awareness.

Meski demikian, potensi yang sama juga dapat dilakukan terhadap pengembangan metode, platform, prototipe, software, dan framework berbasis AI yang mendukung proses security management, defense, data privacy concern, dan decision making. Bidang atau bagian ini belum banyak dikerjakan jika dilihat dari hasil mapping review, sehingga ke depannya peluang untuk mengerjakan bidang-bidang ini cukup besar, termasuk juga mengkolaborasikan antar bidang (misalkan: edukasi dan data privacy concern).

3.3. Metode AI yang Digunakan

Untuk mengetahui metode AI yang digunakan pada cyber security untuk meningkatkan security awareness, dilakukan pendataan terhadap 37 paper. Hasil pemetaan ditampilkan pada Tabel 3. dan grafik ditampilkan dalam bentuk chart pada Gambar 5.

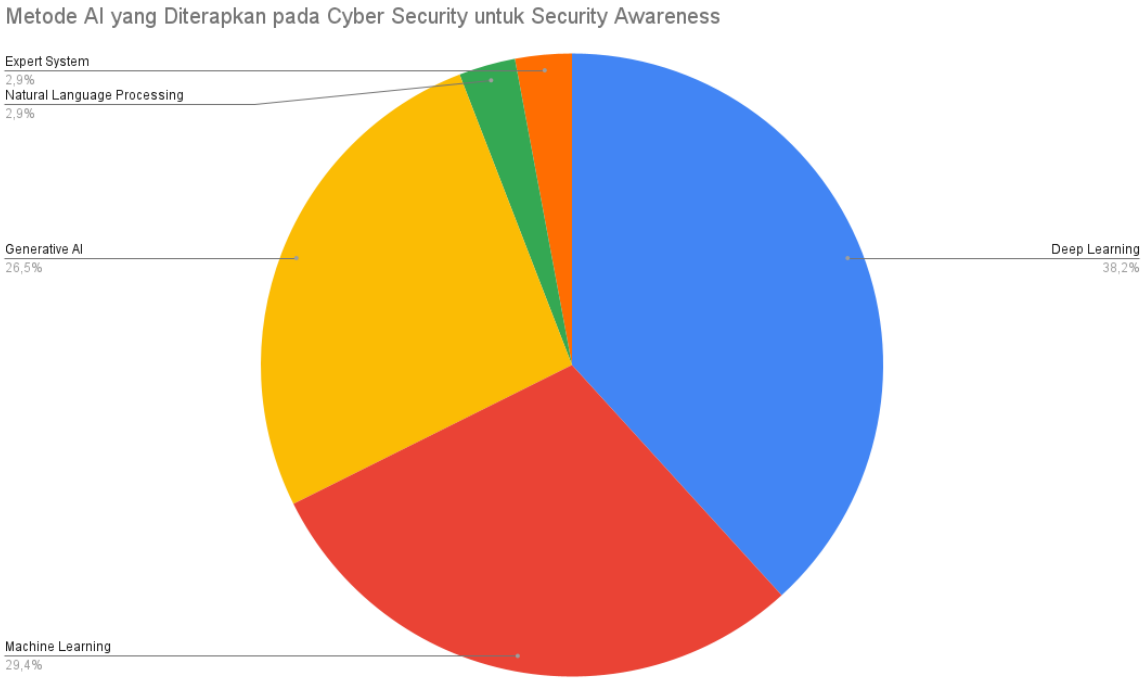
Tabel 3. Metode AI yang Diterapkan pada Cyber Security untuk Security Awareness

Penerapan AI	Paper	Jumlah	Persentase
Deep Learning	[11],[12],[13],[14],[15],[16],[18],[19],[20],[21],[22],[25],[26],[27],[28],[32],[35],[36],[38],[39],[41],[42],[43],[44],[45],[47]	26	70,2%
Machine Learning	[12],[13],[17],[23],[24],[29],[30],[31],[33],[34],[37],[38],[39],[40],[41],[42],[44],[45],[46],[47]	20	54,1%
Generative AI	[12],[13],[14],[15],[18],[20],[21],[22],[27],[35],[36],[39],[41],[42	18	48,6%

Penerapan AI	Paper	Jumlah	Persentase
	],[43],[44],[45],[47]		
Natural Language Processing	[12],[13]	2	5,4%
Expert System	[12],[13]	2	5,4%

Berdasarkan Tabel 3. dan Gambar 5., metode AI yang paling banyak diterapkan pada cyber security untuk security awareness adalah Deep Learning (70,2%), disusul oleh Machine Learning (54,1%) dan Generative AI (48,6%). Dalam jumlah yang sangat sedikit, beberapa paper ada yang menggunakan metode AI berupa Natural Language Processing (NLP) dan Expert System.

Hal ini menunjukkan bahwa Deep Learning, Machine Learning, dan Generative AI adalah tiga metode AI yang paling banyak digunakan dalam ranah penelitian saat ini, termasuk juga pada bidang cyber security. Hal ini menjadikan potensi dan peluang besar untuk ke depannya melakukan penelitian terkait penerapan AI berupa Deep Learning, Machine Learning, maupun Generative AI untuk diterapkan pada bidang cybr security, khususnya meningkatkan security awareness



Gambar 5. Chart metode AI yang diterapkan pada cyber security untuk security awareness

4. Kesimpulan

Berdasarkan hasil mapping review yang telah dilakukan untuk kurun waktu publikasi 2014 hingga 2024, diperoleh kesimpulan bahwa pemetaan publikasi terkait pemanfaatan AI pada cyber security untuk meningkatkan security awareness paling banyak dilakukan pada tahun 2024, di mana trend penerapan AI pada cyber security untuk meningkatkan security awareness terbanyak pada edukasi/pelatihan/training dan metode AI yang paling diterapkan pada cyber security untuk mendukung security awareness adalah Deep Learning.

Berdasarkan hal ini, sangat besar potensi ke depannya untuk melakukan penelitian mengenai pemanfaatan AI pada cyber security untuk meningkatkan security awareness di sisi edukasi/pelatihan/training dengan metode AI berupa Deep Learning. Penulis memberikan rekomendasi untuk memanfaatkan tren dan metode terbanyak ini sebagai acuan penelitian ke depannya yang dapat dilakukan oleh peneliti yang berminat d bidang AI dan cyber security. Ke depannya, penulis akan melanjutkan penelitian ini berupa desain dan pengembangan prototipe berbasis AI dengan metode Deep Learning terkait edukasi cyber security untuk meningkatkan security awareness.

Ucapan Terimakasih

Terima kasih penulis sampaikan kepada Universitas Udayana atas dukungan terhadap penelitian ini melalui hibah penelitian DIPA PNBP Universitas Udayana TA-2024.

Daftar Rujukan

[1] Badan Siber dan Sandi Negara (BSSN), 2023. Lanskap Keamanan Siber Indonesia 2023. [Online] (Updated 10 Des 2023). Tersedia di: https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf [Accessed 25 September 2024].

[2] Tashfiq, R., et al., 2021, Human Factors in Cybersecurity: A Scoping Review. 12th Int. Conf. Adv. Inf. Technol. IAIT2021 2021, 2021, doi: https://doi.org/10.1145/3468784.3468789.

[3] Quintero, B., Santiago, and Angel M.R., 2020, A New Proposal on the Advanced Persistent Threat: A Survey. Applied Sciences 10, no. 11: 3874. https://doi.org/10.3390/app10113874
[4] Yuliana, Y., 2022. The Importance of Cybersecurity Awareness for Children. Lampung J. Int. Law 4, 39–46. https://doi.org/10.25041/lajil.v4i1.2526
[5] Balsano, C, et al., 2023. Artificial Intelligence and liver: Opportunities and barriers. Dig. Liver Dis. 55, 1455–1461. https://doi.org/10.1016/j.dld.2023.08.048a
[6] Ramanpreet K., Dusan G., and Tomaz K., 2023, Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, Vol.97, pp.1566-2535.
[7] National Institute of Standards and Technology (NIST), 2024. The NIST Cybersecurity Framework (CSF) 2.0. [Online] (Updated 26 Feb 2024). Tersedia di: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf [Accessed 25 September 2024].
[8] Maryam A.N., Faisal M.N., Rana S. and Lamay B.S., 2022, A systematic mapping review exploring 10 years of research on supply chain resilience and reconfiguration, International Journal of Logistics Research and Applications, Volume 25, 2022, Issue 8. https://doi.org/10.1080/13675567.2021.1893288
[9] Kiki N.I.S., Yusuf S.N., 2023, Systematic Mapping Study Terhadap Penerapan System Usability Scale Untuk Evaluasi Tingkat Kegunaan Perangkat Lunak. Seminar Riset Mahasiswa Computer and Electrical (SERIMA-CE), Vol.1, No.1.
[10] Armauliza S., 2018, Aplikasi Systematic Mapping Review Sebagai Upaya Pengukuran Efektivitas Pembangunan Desa Pesisir Natuna. JIP (Jurnal Ilmu Pemerintahan): Kajian Ilmu Pemerintahan dan Politik Daerah, Vol.3, No.2. https://doi.org/10.24905/jip.3.2.2018.149-170
[11] Xiangying L., et al., 2024. Application of Artificial Intelligence Technology in Electromechanical Information Security Situation Awareness System, Scalable Computing Practice and Experience, Vol.25, No.1. pp. 127-136. DOI: 10.12694/scpe.v25i1.2280
[12] Ayobami P.O, et al., 2024, Leveraging AI-driven training programs for enhanced organizational security awareness, 1 Department of Computer Science, Western Illinois University, United States of America. International Journal of Science and Research Archive, Vol.13, No.1. pp.301-311. DOI: https://doi.org/10.30574/ijsra.2024.13.1.1649
[13] Shadi J., Jeremy M., Zeina B., 2024, AI-Driven Customized Cyber Security Training and Awareness, in 2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC). DOI: 10.1109/ICAIC60265.2024.10433829
[14] Schreiber, A., and Schreiber, I., 2024, Bridging knowledge gap: the contribution of employees awareness of AI cyber risks comprehensive program to reducing emerging AI digital threats. Information and Computer Security. https://doi.org/10.1108/ICS-10-2023-0199
[15] Anrie S., et al., 2024, Enhancing Personal Data Security Awareness and Vigilance on Social Media Platforms. ABDIMAS: Jurnal Pengabdian Masyarakat, Vol.7, No.2, pp.650–654. https://doi.org/10.35568/abdimas.v7i2.4700
[16] Michał I., 2024, Secuity Management in the Face of Civilizational Awareness of the Digital World: a Theoretical Approach, Scientific Papers of Silesian University of Technology, Organization and Management Series, 197. http://dx.doi.org/10.29119/1641-3466.2024.197.9
[17] Akor, A., et al., 2024. Cybersecurity Awareness: Leveraging Emerging Technologies in the Security and Management of Libraries in Higher Education Institutions. Southern African Journal of Security. https://doi.org/10.25159/3005-4222/16671.a
[18] Loh, P.K.K., Lee, A.Z.Y., and Balachandran, V., 2024, Towards a Hybrid Security Framework for Phishing Awareness Education and Defense. Future Internet, Vol.16, No.86. https://doi.org/10.3390/fi16030086
[19] Amreen A.M. Sharif, and Jaflah A., 2024, Development of Cyber Security Awareness and Education Framework. International Journal of Computing and Digital Systems. http://dx.doi.org/10.12785/ijcds/XXXXXX
[20] Adib H., Mohamed K.A., and Mustafa A.A., 2024, Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges and future research directions. Expert Systems with Applications, Vol.240, https://doi.org/10.1016/j.eswa.2023.122442.
[21] Ahmed M.A., 2024, Behind the digital veil: decoding the influence of HR training oninformation security awareness in Saudi Arabia. Cogent Business and ManageMent, VoL.11, no.1. https://doi.org/10.1080/23311975.2024.2395430
[22] Mateo S., 2024, Enhancing Security in Industrial Application Development: Case Study on Self-Generating Artificial Intelligence Tools. Appl. Sci, 14, 3780. https://doi.org/10.3390/app14093780
[23] Mitesh G.P., et al., 2023, Benefits Of Using Cyber Security Automation With The Advent Of Artificial Intelligence And Machine Learning. Educational Administration: Theory and Practice, Vol.30, No.1, https://doi.org/10.53555/kuey.v30i1.7166
[24] Merve, O.O., et al., 2024, A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. IEEE Access. DOI: 10.1109/ACCESS.2024.3355547
[25] Angafor, G.N., Yevseyeva, I. and Maglaras, L., 2024, Securing the remote office: reducing cyber risks to remote working through regular security awareness education campaigns. Int. J. Inf. Secur., Vol.23, pp.1679–1693. https://doi.org/10.1007/s10207-023-00809-5
[26] Saif A.D.Q., et al., 2024, Navigating Cybersecurity Training: A Comprehensive Review, arXiv:2401.11326, https://doi.org/10.48550/arXiv.2401.11326
[27] Aized A.S., et al., 2023, Securing the Internet of Things: A Comprehensive Review of Security Challenges and Artificial Intelligence Solutions, Foundation University Journal of Engineering and Applied Sciences, Vol 4 No 2. DOI: https://doi.org/10.33897/fujeas.v4i2.779
[28] Al F.H.H.M., 2024, Awareness of cyber security aspects in distance education. Journal of Pedagogical Sociology and Psychology, Vol.6, No.1, pp. 77-88. https://doi.org/10.33902/jpsp.202424403
[29] Penghao L., et al., 2024, Enhancing Security in DevOps by Integrating Artificial Intelligence and Machine Learning. JTPES, Vol.4, No.02. DOI: https://doi.org/10.53469/jtpes.2024.04(02).05
[30] Fadhila T., et al., 2024, Advancing UAV security with artificial intelligence: A comprehensive survey of techniques and future directions. Internet of Things, Volume 27. https://doi.org/10.1016/j.iot.2024.101281
[31] Morgan D., et al., 2024, Information Security Awareness in the Insurance Sector: Cognitive and Internal Factors and Combined Recommendations. Information, Vol.15, No.8. https://doi.org/10.3390/info15080505
[32] Richard M., Jacob K., and Thomas L., 2024, SoK: How Artificial-Intelligence Incidents Can Jeopardize Safety and Security. In Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES '24). https://doi.org/10.1145/3664476.3664510
[33] David K., et al., 2023, A Survey and Perspective on Artificial Intelligence for Security-Aware Electronic Design Automation. ACM Trans. Des. Autom. Electron. Syst. 28, 2, Article 16. https://doi.org/10.1145/3563391
[34] Al M., Alaa A., and Areej., 2023, Machine-Learning-based User Behavior Classification for Improving Security Awareness Provision. International Journal of Advanced Computer Science and Applications, Vol.14, Iss.8. DOI:10.14569/IJACSA.2023.0140819
[35] Sunriz I., et al., 2023, Artificial Intelligence for CyberSecurity: Impact, Limitations, and Future Research Directions. Journal of Emerging Trends and Novel Research (JETNR), Volume,1, Issue.12.
[36] Shchavinsky, Y.V., et al., 2023, Application of Artificial Intelligence for Improving Situationl Training of Cybersecurity Specialists, Information Technologies and

Learning Tools, Vol.97, Iss.5. pp.215-226. DOI:10.33407/itlt.v97i5.5424

[37] Dinesh K., et al., 2023, Phishing Detection Implementation using Databricks and Artificial Intelligence. International Journal of Computer Applications, Volume 185, No.11. DOI: 10.5120/ijca2023922764

[38] Mazhar, T., et al., 2023, Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence. Brain Sci., Vol.13, No.683. https://doi.org/10.3390/brainsci13040683

[39] L. Zhou, 2022, Research on University Security Platform Based on Artificial Intelligence. in 3rd International Conference on Electronic Communication and Artificial Intelligence (IWECAI), Zhuhai, China, pp.297-300. doi: 10.1109/IWECAI55315.2022.00063.

[40] Trim, P.R.J., and Yang I.L., 2022. Combining Sociocultural Intelligence with Artificial Intelligence to Increase Organizational Cyber Security Provision through Enhanced Resilience. Big Data and Cognitive Computing 6, no.4. https://doi.org/10.3390/bdcc6040110

[41] Binny N., et al., 2022, Survey and State of the Art: The impacts of artifcial intelligence techniques in augmentation of cybersecurity: a comprehensive review. Complex and Intelligent Systems, 8. https://doi.org/10.1007/s40747-021-00494-8

[42] Al A.B.O., Alsuwat H., and Alsuwat, E., 2021, Human Factor and Artificial Intelligence: For future software security to be invincible, a confronting comprehensive survey. International Journal of Computer Science and Network Security, Vol.21, No.6. pp.245-251. doi: 10.22937/IJCSNS.2021.21.6.32.

[43] Gasiba T.E., et al., 2021, Raising Security Awareness Using Cybersecurity Challenges in Embedded Programming Courses, in International Conference on Code Quality (ICCQ), Moscow, Russia, pp. 79-92. doi: 10.1109/ICCQ51190.2021.9392965.

[44] Mehra A., and Badotra S., 2021, Artificial Intelligence Enabled Cyber Security, in 6th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India. pp. 572-575. doi: 10.1109/ISPCC53510.2021.9609376.

[45] Gasiba E.T., Lechner U., and Pinto A.M., 2020, Sifu: a cybersecurity awareness platform with challenge assessment and intelligent coach. Cybersecur, Vol.3, No.24. https://doi.org/10.1186/s42400-020-00064-4

[46] Hongqin Z., 2019, Research on Information Security Situation Awareness System Based on Big Data and Artificial Intelligence Technology, in 11th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), Qiqihar, China. pp.568-573. doi: 10.1109/ICMTMA.2019.00131

[47] Li, J., 2018, Cyber security meets artificial intelligence: a survey. Frontiers Inf Technol Electronic Eng, Vol.19. pp.1462-1474. https://doi.org/10.1631/FITEE.1800573