SYSTEMATIC LITERATURE REVIEW: RISIKO PRIVASI DAN KEAMANAN DATA PRIBADI DALAM PENGGUNAAN *ARTIFICIAL INTELLIGENCE* (AI)

Mohamad Ardi[1], Evi Dianti Bintari[2]

[1,2]STMIK PPKIA Tarakanita Rahmawati
[1,2]Jl. Yos Sudarso No.8, Karang Rejo, Tarakan Tengah, Kota Tarakan, 77111, Kalimantan Utara

Email : [1]mohamadardi@ppkia.ac.id, [2]evidianti@ppkia.ac.id

ABSTRAK

Kemajuan teknologi yang canggih diikuti dengan perkembangan zaman yang semakin modern. Berbagai macam teknologi telah diciptakan, salah satunya adalah *Artificial Intelligence* (AI) yang telah membantu kehidupan manusia dalam menjalankan aktivitas di bidang telekomunikasi, transportasi, kesehatan, bahkan bidang pertahanan dan keamanan. AI memerlukan akses data pribadi yang nantinya diolah dan dianalisa oleh teknologi tersebut. Diantara data-data yang dikumpulkan, ada data yang sensitif, yakni data pribadi yang rentan untuk dirusak, dicuri, dan dimanipulasi. Tujuan penelitian ini adalah untuk mengetahui dan memahami berbagai risiko privasi dan keamanan data pribadi dalam penggunaan AI yang sering terjadi beserta solusi untuk mencegahnya. Penelitian ini menerapkan metode *Systematic Literature Review* (SLR). Berdasarkan hasil SLR, peneliti menemukan 200 artikel jurnal *Scopus* dalam pencarian menggunakan *Publish or Perish 8* dan bantuan aplikasi lain seperti *Zotero, Mendeley, VOSviewer,* dan *Microsoft Excel* yang kemudian disaring menjadi 59 artikel terpilih untuk dianalisis secara deskriptif. Hasil penelitian menunjukkan bahwa AI mendapatkan data pribadi secara mudah dari para pengguna teknologi tersebut. Pemahaman akan terjadinya pengambilan data oleh AI yang disebabkan pengiriman data oleh individu melalui berbagai platform merupakan unsur terpenting dalam memastikan keamanan data pribadi. Kesimpulan penelitian ini adalah perlunya pemahaman secara holistik dalam memastikan keamanan data pribadi. Kerjasama antara perusahaan teknologi, masyarakat dan pemerintah diperlukan dalam memastikan akses data pribadi yang diambil oleh AI tidak disalahgunakan dan kepastian dalam keamanan data pribadi.

Keywords: *AI, Keamanan, Data Pribadi, SLR*

ABSTRACT

The advancement of sophisticated technology is followed by the development of an increasingly modern era. Various kinds of technology have been created, one of which is Artificial Intelligence (AI) which has helped human life in carrying out activities in the fields of telecommunications, transportation, health, and even defense and security. AI requires access to personal data which is later processed and analyzed by the technology. Among the data collected, there is sensitive data, namely personal data that is vulnerable to being tampered with, stolen, and manipulated. The purpose of this research is to know and understand the various privacy and security risks of personal data in the use of AI that often occur along with solutions to prevent them. This research applied the Systematic Literature Review (SLR) method. Based on the SLR results, researchers found 200 Scopus journal articles in the search using Publish or Perish 8 and the help of other applications such as Zotero, Mendeley, VOSviewer, and Microsoft Excel which were then filtered into 59 selected articles to be analyzed descriptively. The results showed that AI easily obtained personal data from users of the technology. Understanding the occurrence of data collection by AI due to the transmission of data by individuals through various platforms is the most important element in ensuring personal data security. The conclusion of this research is the need for a holistic understanding in ensuring personal data security. Cooperation between technology companies, society and the government is needed to ensure access to personal data taken by AI is not misused and certainty in personal data security.

Keywords: *AI, Security, Personal Data, SLR*

1. PENDAHULUAN

Artificial Intelligence (AI) atau AI telah menjadi satu fenomena pada lapisan masyarakat global karena pengaruhnya dalam berbagai aspek kehidupan manusia [1][2][3]. Kemajuan pesat dalam AI yaitu sistem perangkat lunak yang dirancang untuk meniru kecerdasan

manusia atau fungsi kognitif telah memicu keyakinan akan potensinya untuk meningkatkan efisiensi pemberian layanan kesehatan dan hasil pasien [4][5][6][7]. Selain itu, penggunaan AI terdapat juga pada bidang telekomunikasi [3][8][9] dan transportasi [8][10][11] yang telah memberikan kemudahan di kehidupan manusia. AI selain digunakan untuk meningkatkan produktifitas manusia juga bisa dimanfaatkan untuk hal-hal yang memunculkan permasalahan. Penggunaan data pribadi seperti foto atau video yang melanggar privasi atau tanpa seizin dari pemilik merupakan hal yang dikhawatirkan [1]. Oleh karena itu, keamanan sistem tidak dapat hanya menggunakan prosedur keamanan tradisional, perlu ditingkatkan, mengingat akan adanya ancaman-ancaman terhadap data, terutama data sensitif yang vital seperti data pribadi pelanggan, yang jika dibobol dapat sangat berbahaya kepada perusahaan, karena memungkinkan perusahaan untuk kehilangan pamor di pasar [12].

Permasalahan yang ada adalah perlunya kepastian keamanan akan data pribadi yang diakses oleh AI agar tidak terjadi penyalahgunaan data seperti misalnya penjualan data pribadi, pengiriman data atau informasi yang tidak benar (*hoaks*) dan eksploitasi data. Penelitian sebelumnya telah melakukan identifikasi akan kekhawatiran masalah keamanan data yang mengancam kebebasan manusia. Tujuan dari penelitian ini adalah untuk mengetahui dan memahami berbagai risiko privasi dan keamanan data pribadi dalam penggunaan AI yang sering terjadi beserta solusi untuk mencegahnya. Penelitian ini menerapkan metode *Systematic Literature Review* (SLR) dengan data yang digunakan dalam penelitian adalah artikel jurnal Scopus yang diterbitkan antara tahun 2018 dan 2022.

2. TINJAUAN PUSTAKA

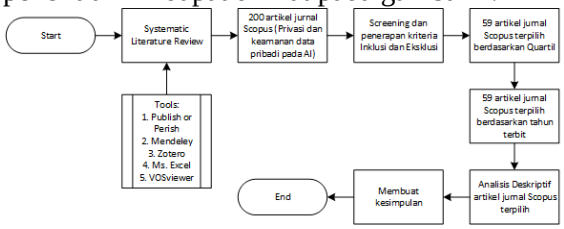
Pada era digital yang terus berkembang pesat, teknologi AI telah menjadi salah satu inovasi terpenting yang memiliki potensi besar dalam mempengaruhi berbagai aspek kehidupan manusia. AI mengacu pada kemampuan mesin untuk meniru atau meniru kecerdasan manusia, termasuk kemampuan untuk belajar, memecahkan masalah, mengambil keputusan, dan berinteraksi dengan lingkungan mereka. AI telah diterapkan dalam berbagai sektor, seperti kesehatan, transportasi, finansial, manufaktur, dan banyak lagi, dengan tujuan meningkatkan efisiensi, produktivitas, dan kualitas hidup manusia. Namun, bersamaan dengan potensi yang menjanjikan, penggunaan AI juga membawa ancaman dan peluang yang perlu dipahami dengan baik oleh masyarakat. Keberadaan AI telah mempengaruhi lapangan kerja, dengan otomatisasi menggantikan pekerjaan manusia dalam beberapa kasus. Selain itu, ada kekhawatiran tentang privasi dan keamanan data, karena AI dapat mengumpulkan, menganalisis, dan menginterpretasikan data pribadi dalam skala yang belum pernah terjadi sebelumnya. Dalam hal ini, perlindungan data dan kebijakan privasi menjadi penting untuk mencegah penyalahgunaan dan pelanggaran privasi yang tidak diinginkan [13].

Privasi dapat diartikan sebagai hak individu untuk mempertahankan informasi pribadi dari akses yang tidak diinginkan atau tidak sah. privasi dapat dijelaskan sebagai "keadaan di mana individu memiliki kendali atas informasi pribadi mereka dan dapat memutuskan apakah, kapan, dan bagaimana informasi itu akan dibagi dengan orang lain". Dalam menjaga keamanan data pribadi, teknologi seperti enkripsi dan tanda tangan digital dapat digunakan untuk melindungi data dari ancaman dan serangan. Namun, implementasi teknologi ini membutuhkan sumber daya yang cukup dan keahlian teknis yang diperlukan. Dalam hal identifikasi dan keamanan data pribadi, penting juga untuk mempertimbangkan peraturan privasi dan keamanan data yang berlaku. Di berbagai negara, ada peraturan privasi dan keamanan data yang mengatur pengumpulan, penggunaan, dan penyebaran data pribadi [14].

SLR merupakan sebuah pendekatan penelitian yang mengumpulkan, mengevaluasi, serta mensintesis informasi ilmiah yang relevan dalam bidang studi tertentu. Tujuan dasar dari pemeriksaan SLR adalah untuk menemukan dan menilai secara menyeluruh literatur yang ada untuk menjawab pertanyaan penelitian spesifik. Dengan melakukan SLR yang menyeluruh yang didasarkan pada penelitian sebelumnya, peneliti dan pengembang dapat memperoleh pemahaman yang lebih baik. Penilaian yang menyeluruh juga memungkinkan untuk menemukan celah penelitian, kekurangan, atau kekurangan pengetahuan yang dapat digunakan sebagai dasar untuk penelitian atau kemajuan di sektor ini di masa depan [15].

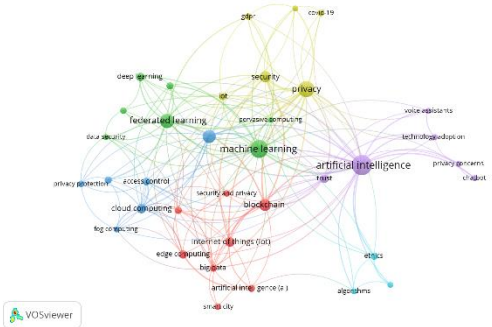
3. METODE PENELITIAN

Metode penelitian yang digunakan adalah SLR seperti yang direkomendasikan oleh Kitchenham dan Charters [16]. Sementara itu, pendekatan kualitatif dalam SLR digunakan merangkum hasil-hasil penelitian yang bersifat deskriptif kualitatif. Adapun flowchart metode penelitian ini dapat dilihat pada gambar 1.



Gambar 1. Flowchart Metode Penelitian

Ada beberapa langkah yang dilakukan peneliti dalam menganalisa dan mendapatkan data kepustakaan sesuai dengan penelitian yang dilakukan. Langkah pertama, yaitu peneliti menggunakan alat bantu atau *tools*, yaitu *Publish or Perish 8*. *Publish or Perish* adalah sebuah *software program* yang digunakan untuk menganalisa dan mendapatkan kembali sitasi akademik dari beberapa sumber seperti, *Google Scholar*, *Scopus*, *Microsoft Academic Search*, dll [17]. Dalam penelitian ini, peneliti mencari artikel jurnal *Scopus* berdasarkan *keywords* "*User Privacy of* AI" terdapat 200 artikel jurnal terkait (pencarian dari tahun 2018 sampai 2022). Setelah itu, peneliti melakukan proses *screening* dan penentuan kriteria dengan bantuan aplikasi *Mendeley* dan *Zotero* untuk mengetahui abstraksi dari 200 literatur tersebut serta *VOSviewer* untuk mengetahui keterkaitan antara *keywords* yang ditemukan seperti pada Gambar 2.



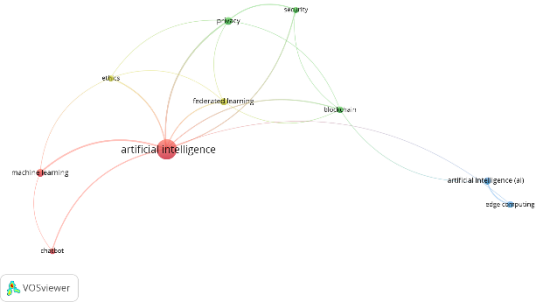
Gambar 2. Hubungan antar 200 literatur *keywords* melalui *VOSviewer*

Berdasarkan *screening* yang telah dilakukan dengan bantuan *VOSviewer*, hubungan antara *artificial intelligence*, *machine learning*, dan *federated learning* menghasilkan keterkaitan dengan banyak *keywords* di antaranya adalah *security*, *privacy*, *internet of things* (iot), *cloud computing*, *access control*, *privacy protection*, *blockchain*, *big data*, dan *edge computing*. Kemudian peneliti membaca abstraksi dan menyaring literatur berdasarkan kriteria inklusi dan eksklusi yang ditunjukan dalam Tabel 1.

Tabel 1. Kriteria Inklusi dan Eksklusi

Penyertaan Kriteria	Jurnal studi yang menggunakan data skala besar dan kecil terkait risiko privasi dan keamanan data pribadi pada AI
	Studi yang membahas tentang AI, keamanan, data pribadi, dan SLR
Pengecualian Kriteria	Studi yang tidak relevan dengan AI, keamanan, data pribadi, dan SLR
	Studi yang mengambil contoh kasus alkohol, narkoba dan obat-obatan terlarang

Dari proses penyaringan tersebut, peneliti mendapatkan 59 literatur terpilih dari jenis jurnal artikel terindeks *Scopus* sebagai data primer dan didukung oleh data sekunder dari buku, jurnal, dan artikel lainnya yang relevan dengan topik. Selanjutnya, peneliti melakukan kembali proses *screening* untuk mengetahui keterkaitan antara *keywords* yang ditemukan seperti pada Gambar 3.



Gambar 3. Hubungan antar 59 literatur *keywords* melalui *VOSviewer*

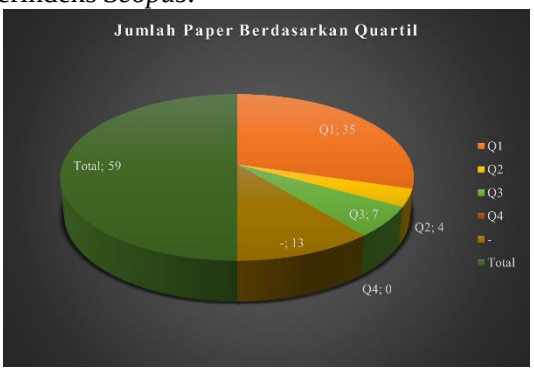
Berdasarkan *screening* kedua yang telah dilakukan dengan bantuan *VOSviewer*, hubungan antara *artificial intelligence* menghasilkan keterkaitan dengan *chatbot*, *machine learning*, *ethics*, *privacy*, *security*, *federated learning*, *blockchain*, *dan edge computing*.

Langkah kedua, yaitu data dari Publish or Perish 8 disimpan dalam format .ris (*RIS/Ref Manager*) dan kemudian di import ke dalam

Mendeley untuk mendapatkan rincian paper tersebut. *Mendeley* adalah sebuah perangkat lunak yang digunakan untuk mengintegrasikan "*citation & reference manager*" ke dalam sebuah jejaring sosial. Dengan jejaring semacam ini, peneliti di berbagai belahan dunia dapat berkolaborasi dan melakukan *sharing* data penelitian [18]. Setelah melakukan *import*, jangan lupa untuk melakukan sinkronisasi di *Mendeley* agar metadata dari 59 jurnal tersebut dapat otomatis diperbaharui.

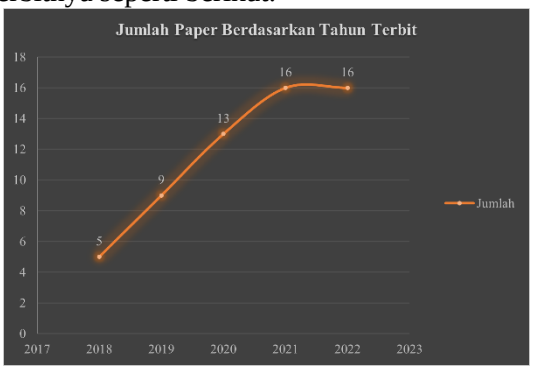
Langkah ketiga, yaitu menyimpan data yang telah disinkronkan di *Mendeley* ke dalam format .xml (*EndNote* XML) agar dapat dibuka di *Microsoft Excel*. Setelah data di *import* ke *Microsoft Excel*, peneliti melakukan penyaringan data dengan menyesuaikan topik penelitian. Karena sumber data berasal dari *Scopus*, peneliti melakukan penyaringan data dengan bantuan *masterscopus*, artinya jurnal yang dikenali adalah jurnal yang telah terindeks *Scopus*. Data *masterscopus* [19] di *import* dalam *sheet* yang berbeda di file *Microsoft Excel* yang sama dengan data *Mendeley* sebelumnya.

Langkah keempat, adalah penyaringan dengan master *Scopus*. Dalam tahap ini jurnal-jurnal yang terindeks maupun tidak terindeks *Scopus* dibagi dalam 4 Kuartil (*Q-ranking of journal*) dimana Q1 merupakan ranking tertinggi dan Q4 adalah ranking terendah. Kuartil ini adalah kategori jurnal ilmiah yang mewakili tingkat kutipan yang diidentifikasi oleh indikator *scientometric*. Jadi, publikasi berkisar dari yang paling direferensikan. Dari 59 jurnal yang didapatkan, untuk Q1, Q2, Q3, dan Q4 masing-masing berjumlah 35 jurnal, 4 jurnal, 7 jurnal, dan 0 jurnal. Dapat dilihat dalam Gambar 4 merupakan hasil penyaringan data dengan *masterscopus* yang sudah terbagi dalam Q1-Q4, dan ada 13 jurnal yang tidak terindeks *Scopus*.



Gambar 4. Klasifikasi Jurnal Berdasarkan *Quartile Master Scopus*

Langkah kelima, adalah penyaringan lanjutan berdasarkan tahun terbit. Dalam Gambar 5, dapat terlihat rincian jumlah jurnal yang diterbitkan di *Scopus* berdasarkan tahun terbitnya seperti berikut.



Gambar 5. Klasifikasi Jurnal Berdasarkan Tahun Terbit

Setelah dilakukan penyaringan data berdasarkan tahun penerbitan, peneliti memutuskan untuk mengambil referensi dari seluruh penelitian dari tahun 2018-2022, tetapi tetap dengan memperhatikan isi dari topik penelitian tersebut. Peneliti membaca dan mengambil poin dari setiap abstrak jurnal terpilih untuk penyusunan isi topik penelitian. Kemudian peneliti juga mengambil data penelitian dari berbagai website yang memuat informasi terkait risiko privasi dan keamanan data pribadi pada AI.

4. PEMBAHASAN

Tindakan yang dilakukan oleh AI dalam melakukan akses data pribadi manusia atau pengguna, adalah permasalahan yang tidak kunjung selesai. Data pribadi tersebut diolah dan dianalisa sehingga oleh pihak tertentu yang memanfaatkan AI dapat digunakan untuk kepentingan yang bisa menguntungkan pihak tersebut namun merugikan pengguna. Data pribadi tersebut menjadi data yang bernilai ekonomis. Data yang diambil tersebut selain dapat diolah dan menghasilkan produk atau jasa yang lebih baik untuk dipasarkan namun juga menjadi pemantau atau monitor akan segala aktivitas pengguna.

AI ketika melakukan akses ke data pribadi, maka akan mengolah dan melakukan analisa prediktif apa yang menjadi perhatian pengguna. AI akan selalu menampilkan konten atau iklan atau informasi berdasarkan analisa prediktif tersebut akan menarik perhatian pengguna. Karena AI memprediksi bahwa hal itu akan segera ditanggapi atau dilihat oleh pengguna

karena menarik perhatiannya. Ini semua berdasarkan sejumlah data yang besar atau *Big Data* yang diproses oleh AI. Mulai dari data akan pertemanan, hubungan antar sesama, keyakinan politik atau agama, riwayat pembelian, data kesehatan atau data Geolocation dikumpulkan oleh AI untuk diolah dan dianalisa sehingga menghasilkan analisa prediktif. Hal inilah yang menjadi kekwatiran atau permasalahan mengenai keamanan dan penggunaan data pribadi.

Di tangan orang atau organisasi yang tidak bertanggung jawab, maka data pribadi tersebut akan dipergunakan untuk dijualbelikan, baik untuk kepentingan ekonomi ataupun politik. Di Amerika Serikat, organisasi yang berada di industri pialang data tumbuh berkembang pesat. CheckPoint, salah satu organisasi yang bergelut di industri pialang data pernah melakukan pelanggaran keamanan data pribadi dengan mengungkap informasi keuangan pribadi sejumlah 163 ribu konsumen.

Permasalahan data pribadi menimbulkan pertanyaan akan etika AI dalam mengumpulkan dan menggunakan data. Penggunaan AI dalam pabrik bisa menimbulkan masalah etika ketika berhubungan dengan data pribadi, diskriminasi, dan keadilan. Pengawasan yang berlebihan terhadap karyawan di organisasi melalui AI menimbulkan perdebatan.

Data pribadi memang mempunyai nilai. Bagi organisasi yang mencari untung, maka dengan memaksimalkan pengolahan data pribadi melalui AI akan menaikkan pendapatan. Teknik segmentasi dan penargetan konsumen oleh organisasi juga bisa dilakukan untuk kegiatan kampanye politik. Profil pemilih dapat dengan mudah diakses oleh AI dari berbagai data yang diambil dari media sosial atau akses data lainnya. Nantinya oleh AI akan diberikan konten atau iklan yang menarik si pengguna agar tetap memilih atau berpindah pilihan akan politiknya.

5. KESIMPULAN

Dalam kesimpulan penelitian ini, temuan utamanya adalah mengetahui bahwa AI adalah temuan teknologi yang tidak bisa dihindarkan dan AI mengambil data pribadi untuk bisa melakukan analisa prediktif. Penelitian ini mengindentifikasi bahwa data pribadi telah terakses oleh AI melalui banyaknya data yang terkumpul di *Big Data*. Terkumpulnya data ini disebabkan oleh kegiatan yang dilakukan oleh individu melalui sosial media atau lokapasar atau berbagai platform lainnya secara aktif dalam mengirimkan data berbentuk video, percakapan/teks, atau suara. Keamanan data pribadi menjadi rentan, karena pengambilan data oleh AI yang dilakukan setiap saat. Hal ini terjadi baik data pribadi individu diambil tanpa persetujuan individu tersebut atau tidak sadar. Tentunya menjadi perdebatan akan etika dari AI mengakses data tersebut dan mengolahnya menjadi nilai bagi organisasi pencari keuntungan atau organisasi politik.

Rekomendasi penelitian selanjutnya adalah eksplorasi lebih lanjut mengenai tindakan yang harus dilakukan oleh perusahaan teknologi, organisasi swasta pencari keuntungan, masyarakat dan tentutnya pihak pemerintah dalam merancang peraturan yang bisa menjaga data pribadi individu. Penelitian selanjutnya juga bisa mengeksplorasi dampak dari diambilnya data pribadi pada kesetaraan politik atau ekonomi pada masyarakat secara menyeluruh. Kesimpulannya, adanya wawasan akan bagaimana AI mengambil dan menggunakan data pribadi dalam era masyarakat modern saat ini yang telah tergantung pada dukungan internet dalam kehidupan sehari-hari. Individu tidak sadar bahwa data pribadi mereka diambil sehingga prilaku akan mereka diketahui lalu direkam dan dianalisa untuk nantinya dijadikan analisa prediktif sehingga menjadi database yang bernilai, bagi suatu organisasi atau lainnya untuk mencapai tujuannya, baik itu secara ekonomi dengan memaksimalkan pendapatan atau politik atau tujuan lainnya.

DAFTAR PUSTAKA

[1] A. M. Soemarno, “Masalah Privasi dan Keamanan Data Pribadi pada Penerapan AI,” *Innov. J. Soc. Sci. Res.*, vol. 3, no. 6, 2023, [Online]. Available: http://j-innovative.org/index.php/Innovative/article/view/7096

[2] N. Rahim, J. Ahmad, K. Muhammad, A. K. Sangaiah, and S. W. Baik, “Privacy-preserving image retrieval for mobile devices with deep features on the cloud,” *Comput. Commun.*, vol. 127, pp. 75–85, 2018, doi: 10.1016/j.comcom.2018.06.001.

[3] P. McEnroe, S. Wang, and M. Liyanage,

"A Survey on the Convergence of Edge Computing and AI for UAVs: Opportunities and Challenges," *IEEE Internet Things J.*, vol. 9, no. 17, pp. 15435–15459, 2022, doi: 10.1109/JIOT.2022.3176400.

[4] H. S. Jocelyn Chew and P. Achananuparp, "Perceptions and Needs of Artificial Intelligence in Health Care to Increase Adoption: Scoping Review," *Journal of Medical Internet Research*, vol. 24, no. 1. 2022. doi: 10.2196/32939.

[5] T. Panch, P. Szolovits, and R. Atun, "Artificial intelligence, machine learning and health systems," *J. Glob. Health*, vol. 8, no. 2, pp. 1–8, 2018, doi: 10.7189/jogh.08.020303.

[6] T. Panch, J. Pearson-Stuttard, F. Greaves, and R. Atun, "Artificial intelligence: opportunities and risks for public health," *Lancet Digit. Heal.*, vol. 1, no. 1, pp. e13–e14, 2019, doi: 10.1016/S2589-7500(19)30002-0.

[7] H. S. J. Chew, W. H. D. Ang, and Y. Lau, "The potential of artificial intelligence in enhancing adult weight loss: A scoping review," *Public Health Nutr.*, vol. 24, no. 8, pp. 1993–2020, 2021, doi: 10.1017/S1368980021000598.

[8] A. Renda *et al.*, "Federated Learning of Explainable AI Models in 6G Systems: Towards Secure and Automated Vehicle Networking," *Inf.*, vol. 13, no. 8, 2022, doi: 10.3390/info13080395.

[9] B. Kuang, A. Fu, W. Susilo, S. Yu, and Y. Gao, "A survey of remote attestation in Internet of Things: Attacks, countermeasures, and prospects," *Comput. Secur.*, vol. 112, 2022, doi: 10.1016/j.cose.2021.102498.

[10] A. Gupta, C. Chakraborty, and B. Gupta, "Medical information processing using smartphone under IoT framework," *Studies in Systems, Decision and Control*, vol. 206. pp. 283–308, 2019. doi: 10.1007/978-981-13-7399-2_12.

[11] L. Meyer-Waarden and J. Cloarec, "'Baby, you can drive my car': Psychological antecedents that drive consumers' adoption of AI-powered autonomous vehicles," *Technovation*, vol. 109, 2022, doi: 10.1016/j.technovation.2021.102348.

[12] D. Prayoga, F. Hayati, H. A. Y. Putra, I. N. Rizki, and F. Fitroh, "Risiko Keamanan Data Pribadi Pelanggan Dalam Penggunaan Big Data," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 5, no. 3, pp. 459–463, 2022, doi: 10.32672/jnkti.v5i3.4381.

[13] S. Masrichah, "Ancaman Dan Peluang Artificial Intelligence (AI)," *J. Pendidik. dan Sos. Hum.*, vol. 3, no. 3, pp. 83–101, 2023, [Online]. Available: https://doi.org/10.55606/khatulistiwa.v3i3.

[14] I. Cahyanto, "Privacy Challenges in Using Wearable Technology in Education Literature Review," *Formosa J. Appl. Sci.*, vol. 2, no. 6, pp. 909–928, 2023, doi: 10.55927/fjas.v2i6.4272.

[15] K. Wulandari, L. H. Sabilissalam, and Y. Sugiarti, "SYSTEMATIC LITERATURE REVIEW : PENELITIAN USER INTERFACE (UI) PADA PENGEMBANGAN APLIKASI SELULER (MOBILE)," *J. Inf. Interaktif*, vol. 8, no. 3, pp. 80–88, 2023.

[16] Keele S, "Guidelines for performing systematic literature reviews in software engineering," *Tech. report, Ver. 2.3 EBSE Tech. Report. EBSE*, vol. 2, Jan. 2007.

[17] A. W. Harzing, "Publish or Perish," 2007. https://harzing.com/resources/publish-or-perish (accessed Jan. 03, 2023).

[18] J. Fadhilah, C. A. A. Layyinna, R. Khatami, and F. Fitroh, "Pemanfaatan Teknologi Digital Wallet Sebagai Solusi Alternatif Pembayaran Modern: Literature Review," *J. Comput. Sci. Eng.*, vol. 2, no. 2, pp. 89–97, 2021, doi: 10.36596/jcse.v2i2.219.

[19] Scimago, "Journal Rankings on Scopus," 2021. https://www.scimagojr.com/journalrank.php (accessed Jan. 03, 2024).