Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.2023107341
Vol. 10, No. 6, Desember 2023, hlm. 1185-1196 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 36/E/KPT/2019 e-ISSN: 2528-6579

SURVEI PENELITIAN METODE KECERDASAN BUATAN UNTUK MENDETEKSI ANCAMAN TEKNOLOGI SERANGAN SIBER

Eza Yolanda Fitria[*1], Kusprasapta Mutijarsa[2]

[1,2] Institut Teknologi Bandung, Bandung
Email: [1]23221118@mahasiswa.itb.ac.id, [2]kusprasapta.mutijarsa@itb.ac.id
[*]Penulis Korespondensi

(Naskah masuk: 05 Juni 2023, diterima untuk diterbitkan: 27 November 2023)

Abstrak

Keamanan siber merupakan isu penting di era modern seperti sekarang ini. Serangan siber yang semakin beragam terus bermunculan. Teknik dan metode baru *machine learning* dan *deep learning* terus dikembangkan oleh banyak peneliti untuk menangani serangan siber. Selain teknik baru, berbagai jenis *dataset* baru terkait serangan siber juga turut berkembang. Permasalahan muncul ketika banyaknya teknik atau metode yang ada belum tentu tepat menangani berbagai jenis serangan siber. Begitupun sebaliknya, belum tentu berbagai jenis serangan siber dapat ditangani hanya dengan menggunakan teknik atau metode tertentu saja. Tujuan penelitian ini adalah memetakan teknik-teknik dan metode kecerdasan buatan untuk mendeteksi ancaman teknologi serangan siber dalam bentuk *Systematic Literature Review* (*SLR*). Pada penelitian ini teknik dan metode *machine learning* maupun *deep learning* dievaluasi untuk dapat menangani jenis serangan siber tertentu dengan tepat. Berbagai *dataset* yang dapat digunakan untuk eksperimen juga dieksplorasi. Jenis serangan siber yang dibahas pada penelitian ini difokuskan jenis serangan pada sistem *host* dan serangan pada lapisan keamanan jaringan. Pada penelitian *SLR* sebelumnya, hal-hal tersebut dibahas secara terpisah atau bahkan salah satunya saja sehingga dalam penelitian ini perlu dibangun kembali *SLR* yang bisa mengisi kekurangan pada penelitian *SLR* sebelumnya. Originalitas penelitian ini terletak pada analisis teknik atau metode kecerdasan buatan yang secara spesifik tepat untuk menangani jenis serangan siber tertentu. Terdapat total 44 *paper* survei yang diulas, diterbitkan antara tahun 2018 hingga 2023. Dari keseluruhan *paper* tersebut, 30 *paper* membahas penggunaan teknk *machine learning* dan *deep learning*. Kemudian, 19 *paper* yang membahas penggunaan *dataset* dan 13 *paper* membahas peluang penelitian masa depan. Terakhir, 5 *paper* yang membahas terkait *tools.* Hasil dari penelitian ini diharapkan dapat berkontribusi dalam memberikan wawasan baru di dunia keamanan siber untuk membuka peluang penelitian masa depan, terutama bagi para peneliti pemula yang ingin melakukan riset di bidang keamanan siber.

Kata kunci: Keamanan Siber, Serangan Siber, Kecerdasan Buatan, *Machine Learning, Deep Learning*, *Dataset.*

RESEARCH SURVEY ON ARTIFICIAL INTELLIGENCE METHODS FOR DETECTING CYBERATTACK TECHNOLOGY THREATS

Abstract

Cybersecurity is an essential issue in today's modern era. An increasingly diverse range of cyberattacks continues to emerge. Many researchers continue to develop new techniques and methods for machine learning and deep learning to deal with cyberattacks. In addition to new techniques, various types of new datasets related to cyberattacks are also developing. Problems arise when the many existing techniques or methods are not appropriate for dealing with various types of cyberattacks. Vice versa, it is not certain that various types of cyberattacks can be handled only using specific techniques or methods. This research aims to map the techniques and methods of artificial intelligence to detect cyber-attack technology threats in the form of a Systematic Literature Review (SLR). In this research, machine learning and deep learning techniques and methods are evaluated to be able to handle certain types of cyberattacks properly. Various datasets that can be used for experiments are also explored. The types of cyberattacks discussed in this study focus on attacks on the host system and the network security layer. In previous SLR research, these matters were discussed separately or even just one of them. In this study, it was necessary to rebuild the SLR, which could fill the deficiencies in the previous SLR research. The originality of this research lies in the analysis of artificial intelligence techniques or methods that are specifically appropriate for dealing with certain types of cyberattacks. A total of 44 reviewed survey papers were published between 2018 and 2023. Of all these, 30 papers discuss machine learning and deep learning techniques. Then, 19 papers examine the use of datasets, 13 papers discuss future research opportunities, and five papers discuss developing tools. The results of this research are expected to contribute to providing new insights

into the world of cybersecurity to open future research opportunities, especially for novice researchers who wish to conduct research in the field of cybersecurity.

Keywords: *Cybersecurity, Cyberattacks, Artificial Intelligence, Machine Learning, Deep Learning, Datasets*

1. PENDAHULUAN

Penjahat siber semakin hari semakin hebat taktiknya dalam mencari celah kerentanan suatu sistem, *website,* ataupun aplikasi. Munculnya berbagai jenis serangan siber baru adalah bukti nyata dari kinerja para penjahat siber. Hal ini tentunya menjadi ancaman tersendiri bagi pengguna karena dapat menyebabkan berbagai macam dampak buruk seperti bocornya *data* penting, kerusakan sistem komputer, kehilangan koneksi jaringan dan lain-lain. Untuk mencegah dampak buruk ini terjadi maka para pakar keamanan siber berusaha mengembangkan berbagai metode dengan memanfaatkan teknologi kecerdasan buatan atau yang biasa disebut *artificial intelligence* (AI) termasuk di dalamnya yang biasa dikenal dengan *machine learning* dan *deep learning.*

Teknologi kecerdasan buatan berperan penting dalam pembangunan sosial dan ekonomi, serta paling cepat berkembang, paling banyak digunakan dan paling berpengaruh di dunia hari ini. Namun pada saat yang sama juga, teknologi informasi membawa ancaman terhadap dunia keamanan jaringan secara keseluruhan yang membuat sistem informasi juga menghadapi tantangan besar, serta mempengaruhi stabilitas dan perkembangan masyarakat (He, Shi, Huang, Chen, & Tang, 2022). Kecerdasan buatan adalah suatu jenis komputerisasi versi kecerdasan manusia, karena cara kerja kecerdasan buatan yaitu dengan belajar berulang-ulang layaknya manusia (Sagar, Niranjan, Kashyap, & Sachin, 2019).

Perkembangan berbagai teknik atau metode AI terus diikuti juga dengan perkembangan serangan siber baru yang terus muncul. Banyaknya teknik atau metode AI yang ada belum tentu tepat menangani berbagai jenis serangan siber. Begitupun sebaliknya, berbagai jenis serangan siber yang muncul belum tentu dapat ditangani dengan teknik atau metode tertentu saja. Penelitian ini bertujuan memetakan teknik dan metode AI untuk mendeteksi ancaman teknologi serangan siber dalam bentuk *Systematic Literature Review* (*SLR*). Pada penelitian *SLR* sebelumnya, hal-hal terkait jenis serangan siber, metode AI, maupun *dataset* dibahas secara terpisah atau hanya dibahas salah satunya saja. Dengan demikian, *SLR* perlu dibangun kembali untuk melengkapi kekurangan pada penelitian *SLR* sebelumnya. Untuk melakukan eksperimen, para peneliti juga membutuhkan *dataset* yang relevan sehingga perlu dilakukan analisis *dataset*. Pada penelitian ini, berbagai *dataset* juga dieksplorasi. Originalitas penelitian ini terletak pada analisis teknik atau metode kecerdasan buatan yang secara spesifik tepat untuk menangani jenis serangan siber tertentu.

Keamanan siber mengacu pada tindakan pencegahan yang dirancang untuk melindungi ketersediaan dan integritas pertukaran informasi. Langkah-langkah keamanan informasi biasanya melindungi fakta virtual dari sumber ilegal yang mengakses masuk, manipulasi, pengubahan, atau penghancuran baik pada teknologi perangkat keras maupun lunak (Goyal & Sharma, 2019). Sangat penting menjaga suasana keamanan yang layak dan bebas dari segala bentuk pelanggaran untuk terus menggunakan layanan komputer juga ditekankan dalam penelitian (Waguie & Al-Turjman, 2022).

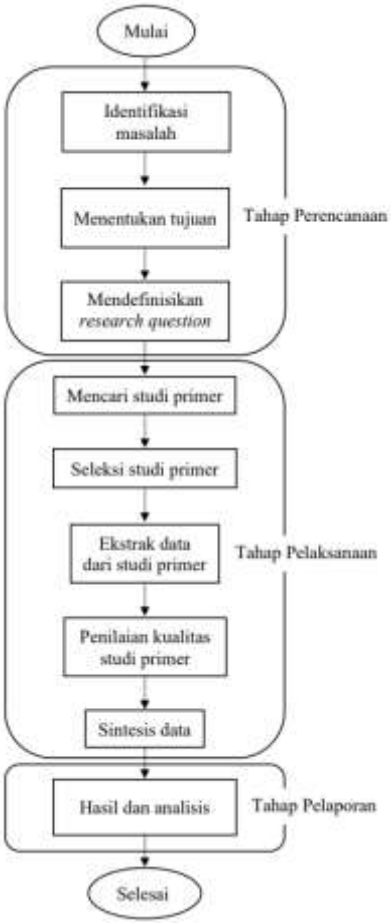
Hasil dari penelitian survei ini diharapkan dapat memberikan kontribusi sebagai bahan referensi ataupun acuan utama para peneliti lain di bidang keamanan siber, terutama dalam hal memilih metode atau teknik *machine learning* mana yang terbaik untuk diterapkan dalam menghadapi kategori serangan siber tertentu. Dengan demikian dampak buruk dari ancaman siber ini dapat diminimalisir dan para pengguna dapat menggunakan layanan teknologi secara lebih leluasa, aman, dan nyaman.

2. METODE PENELITIAN

Tahap pelaksanaan SLR terdiri dari 3 (tiga) bagian, yaitu perencanaan, pelaksanaan, dan pelaporan, seperti diperlihatkan pada Gambar 1. Pada tahap perencanaan dilakukan proses identifikasi masalah sehingga diketahui tujuan pentingnya melakukan penelitian ini. Tahap perencanaan menghasilkan susunan *research question* (*RQ*) untuk menjawab tujuan penelitian.

Tahap pelaksanaan melakukan pencarian studi primer menggunakan kata kunci dalam *database*, menyeleksinya, mengekstrak *data* dari studi primer tersebut, memberikan penilaian terhadap kualitas studi primer, terakhir melakukan sintesis *data* berdasarkan studi primer terpilih. Tahap *SLR* yang terakhir yaitu tahap pelaporan hasil *literature review* ditunjukkan pada bagian 3 dari tulisan ini, mencakup hasil dan analisis dari studi primer akhir, gambaran umum studi dan jawaban dari setiap *RQ*.

Tahapan pelaksanaan *SLR* pada Gambar 1 dibawah ini diuraikan secara rinci pada pembahasan berikutnya.



Gambar 1. Tahap pelaksanaan *SLR*

2.1. Tahap Perencanaan

Tahap perencanaan dilakukan untuk memperoleh *RQ* berdasarkan tujuan penelitian. Setiap topik yang dipilih memiliki kebutuhan yang berbeda, sehingga *research question* (*RQ*) harus ditentukan untuk menjaga fokus *review* yang dirancang. *RQ* adalah permulaan dasar pelaksanaan *SLR* yang digunakan untuk menuntun proses pencarian dan ekstraksi literatur. Analisis dan sintesis *data* sebagai hasil dari *SLR* adalah jawaban dari *RQ* yang ditentukan sebelumnya. *RQ* yang bermanfaat ketika terukur arahnya ke pemahaman terhadap *state-of-the-art research* dari topik penelitian. Tabel 1. menunjukkan *RQ* dan motivasi dalam penelitian ini.

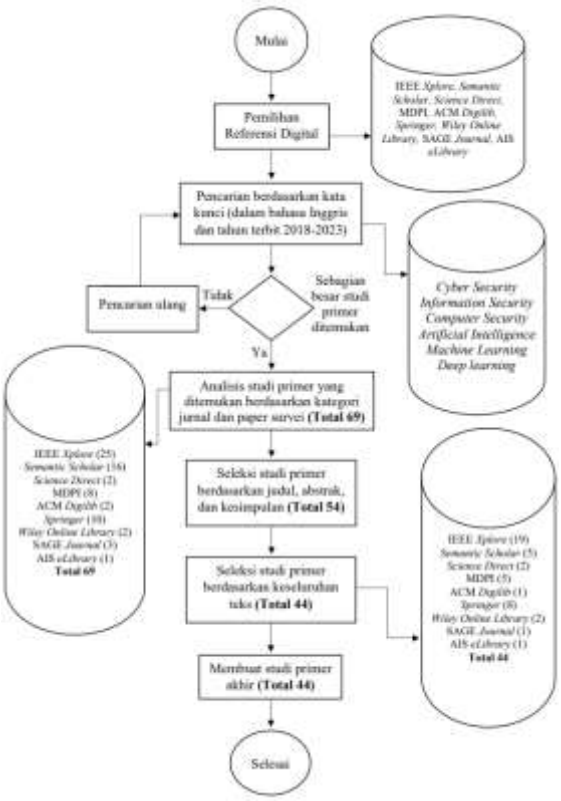
Tabel 1. *Research Question SLR*

No	*Research Question*	Motivasi
1	Apa saja jenis-jenis serangan siber yang bersifat teknis dan sering terjadi?	Identifikasi berbagai jenis serangan siber yang bersifat teknis dan sering terjadi
2	Teknik atau metode apa saja yang ada dalam AI (*artificial intelligence*)?	Identifikasi teknik atau metode yang ada dalam AI (*artificial intelligence*)
3	Teknik atau metode AI (*artificial intelligence*) apa saja yang biasanya digunakan untuk mengatasi masalah keamanan siber?	Identifikasi teknik atau metode AI (*artificial intelligence*) yang biasanya digunakan untuk mengatasi masalah keamanan siber
4	*Dataset* apa yang banyak digunakan pada penelitian AI (*artificial intelligence*) terkait dengan keamanan siber?	Identifikasi *dataset* yang banyak digunakan pada penelitian AI (*artificial intelligence*) terkait dengan keamanan siber
5	Teknik atau metode AI (*artificial intelligence*) mana yang secara spesifik tepat untuk menangani jenis serangan siber tertentu?	Identifikasi teknik atau metode AI (*artificial intelligence*) yang secara spesifik tepat untuk menangani jenis serangan siber tertentu

Jawaban dari *RQ* 1 hingga *RQ* 5 secara sistematis akan dituangkan pada bagian 3 hasil dan analisis. Hal ini akan menunjukkan arah survei dari suatu topik penelitian serta secara tidak langsung dapat membuka peluang penelitian lain dalam keamanan siber.

2.2. Tahap Pelaksanaan

Dalam identifikasi studi, proses yang dilakukan ditunjukkan pada Gambar 2. Terdapat beberapa *database* yang dipilih dan publikasi yang diambil dari masing-masing *database* tersebut. Pencarian dalam *database* juga didasarkan pada kata kunci sesuai dengan topik yang dipilih, kemudian publikasi yang ditemukan disaring kembali berdasarkan beberapa parameter hingga mendapatkan hasil studi akhir yang tepat.



Gambar 2. Desain strategi pemilihan studi

Database yang dipilih dalam penelitian ini yaitu IEEE *Xplore, Semantic Scholar*, *Science Direct*, MDPI, ACM *Digilib, Springer, Wiley Online Library,* SAGE *Journal,* dan AIS *eLibrary* seperti

yang terlihat pada Gambar 2. Awalnya didapatkan 69 *paper* secara keseluruhan dari *database* tersebut, kemudian diseleksi kembali menjadi 54 *paper* saja. Terakhir, total *paper* yang akan dianalisis lebih lanjut sebagai studi primer akhir sebanyak 44 *paper*.

3. HASIL DAN ANALISIS

Dalam menyajikan hasil dan analisis terhadap identifikasi sebanyak 44 studi primer akhir yang membahas tentang keamanan siber, keamanan informasi, dan keamanan komputer yang terkait dengan kecerdasan buatan dan *machine learning* perlu diberikan suatu tinjauan singkat tentang karakteristik umum studi tersebut. Kemudian, setiap pertanyaan penelitian (*RQ* 1-*RQ* 5) akan dijawab dan diuraikan secara sistematis.

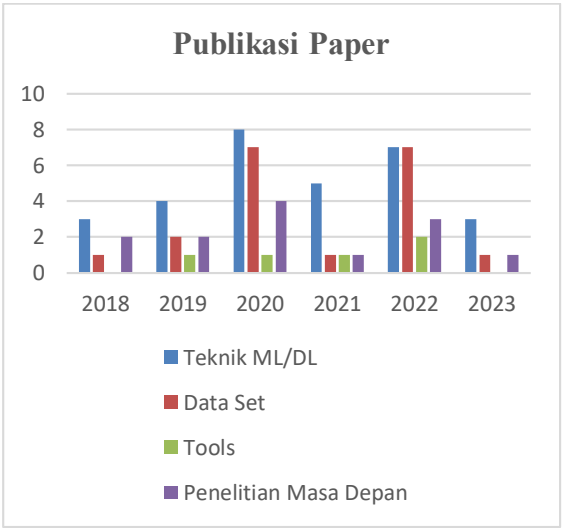
3.1. Gambaran Umum Studi

Terdapat total 44 *paper* survei yang diulas diterbitkan antara tahun 2018 hingga 2023. Dalam tren 5 (lima) tahun terakhir ini, para peneliti seperti ditunjukkan pada Tabel 2 sebagian besar membahas penggunaan teknik *machine learning* dan *deep learning* dengan total 30 *paper*. Kemudian, disusul pembahasan tentang penggunaan *dataset* 19 *paper* dan peluang penelitian masa depan dengan total 13 *paper*. Pembahasan terkait *tools* adalah yang paling sedikit yaitu total 5 *paper*.

Tabel 2. Strategi Evaluasi Studi

Nama	*Paper*/Jurnal	Total
Teknik ML/DL	(Kumar, Singh, & Kumar, 2021) (Farooq & Otaibi, 2018) (Zarandi & Sharifi, 2020) (Shaukat, Luo, Varadharajan, Hameed, & Xu, 2020) (Mishra, Varadharajan, Tupakula, & Pilli, 2019) (Laqtib, Yassini, & Hasnaoui, 2020) (Xin et al., 2018) (Veiga, 2018) (Bagui, Kalaimannan, Bagui, Nandi, & Pinto, 2019) (Larriva-Novo, Vega-Barbas, Villagra, & Sanz Rodrigo, 2020) (Ahmetoglu & Das, 2022) (Barik, Misra, Konar, Fernandez-Sanz, & Koyuncu, 2022) (Abdullahi et al., 2022) (Bécue, Praça, & Gama, 2021) (Yinka-Banjo & Ugot, 2020) (Waqas et al., 2022) (Nguyen & Reddi, 2021) (Yan, Wen, Nepal, Paris, & Xiang, 2022) (de Azambuja et al., 2023) (Sarker et al., 2020) (Sen, Heim, & Zhu, 2022) (Zhimin Zhang et al., 2021) (Dasgupta, Akhtar, & Sen, 2022) (Ibor, Oladeji, Okunoye, & Ekabua, 2020) (Elsisi et al., 2021) (Vinayakumar et al., 2019) (Mari, Zinca, & Dobrota, 2023) (Apruzzese et al., 2023) (Kaja, Shaout, & Ma, 2019) (Tian et al., 2020)	30
Dataset	(Zhibo Zhang, Hamadi, Damiani, Yeun, & Taher, 2022) (Shaukat et al., 2020) (Laqtib et al., 2020) (Yadav, Pathak, & Saraswat, 2020) (Xin et al., 2018) (Bagui et al., 2019) (Larriva-Novo et al., 2020) (Mohd Yusof & Sulaiman, 2022) (Ahmed, Cox, Simpson, & Aloufi, 2022) (Abdullahi et al., 2022) (Bécue et al., 2021) (Ferrag, Shu, Friha, & Yang, 2022) (Sarker et al., 2020) (Sen et al., 2022) (Dasgupta et al., 2022) (Ibor et al., 2020) (Vinayakumar et al., 2019) (Mari et al., 2023) (Tian et al., 2020)	19
Tools	(Zhibo Zhang et al., 2022) (Goyal & Sharma, 2019) (Kumar et al., 2021) (Ahmed et al., 2022) (Shaukat et al., 2020)	5
Peluang Riset Masa Depan	(Zhibo Zhang et al., 2022) (Sagar et al., 2019) (Zarandi & Sharifi, 2020) (Mishra et al., 2019) (Laqtib et al., 2020) (Xin et al., 2018) (Veiga, 2018) (Larriva-Novo et al., 2020) (Mohd Yusof & Sulaiman, 2022) (Truong, Diep, & Zelinka, 2020) (Waqas et al., 2022) (Nguyen & Reddi, 2021) (Kaur, Gabrijelčič, & Klobučar, 2023)	13

Agar lebih terlihat visualisasinya berdasarkan Tabel 2 maka dibuatlah ke dalam bentuk grafik seperti pada Gambar 3 yang menunjukkan hasil bahwa tahun publikasi terbanyak pada penggunaan teknik *machine learning* dan *deep learning* berada pada tahun 2020 sebanyak 8 *paper*. Kemudian untuk penggunaan *dataset* berada pada tahun 2020 dan 2022 sebanyak 7 *paper*, peluang penelitian masa depan berada pada tahun 2020 sebanyak 4 *paper*, dan penggunaan *tools* berada pada tahun 2022 sebanyak 2 *paper*. Pada tahun 2018 dan 2023, tidak terdapat sama sekali publikasi penelitian terkait *tools*.



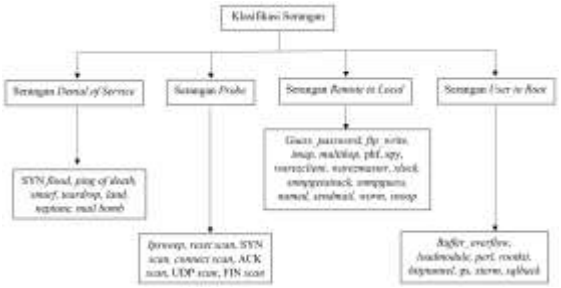
Gambar 3. Grafik publikasi *paper* tahun 2018-2023

3.2. Hasil dan Analisis dari Setiap Research Question

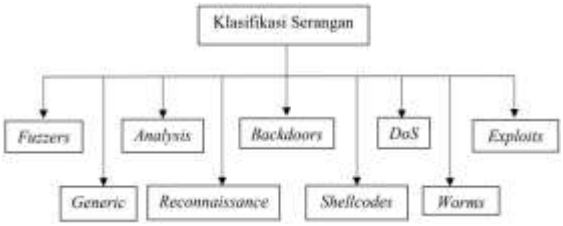
1) Apa saja jenis-jenis serangan siber yang bersifat teknis dan sering terjadi? (*RQ* 1)

Serangan siber dapat dikelompokkan menjadi serangan siber yang bersifat teknis dan serangan siber yang bersifat sosial. Biasanya serangan siber yang bersifat teknis adalah serangan yang terjadi di sistem *host* dan di setiap layer keamanan jaringan, sementara serangan yang bersifat sosial adalah serangan yang termasuk kategori *social engineering* dan *pishing*. Dalam serangan siber yang bersifat sosial ini, faktor manusia (pengguna) berperan penting dalam

mencegah terjadinya serangan. Dalam penelitian ini difokuskan pada pembahasan serangan siber yang bersifat teknis. Menurut penelitian (Zhibo Zhang et al., 2022) beberapa ancaman atau serangan siber yang terdapat di *host* dan di setiap layer keamanan jaringan yang umum dikenal yaitu *malware, spam*, intrusi jaringan, DoS, DGAs, dan botnet. Deteksi intrusi, *malware,* dan *spam* juga disebutkan kembali dalam penelitian (Apruzzese, Ferretti, Marchetti, Colajanni, & Guido, 2018) dan (Shaukat et al., 2020). Dalam penelitian (Mishra et al., 2019) ditekankan bahwa meningkatnya tingkat intrusi di jaringan dan sistem *host* sangat mempengaruhi keamanan siber dan privasi pengguna. Gambar 4. dan gambar 5. menunjukkan kategori serangan berdasarkan *dataset* seperti yang dijelaskan dalam penelitian (Mishra et al., 2019).



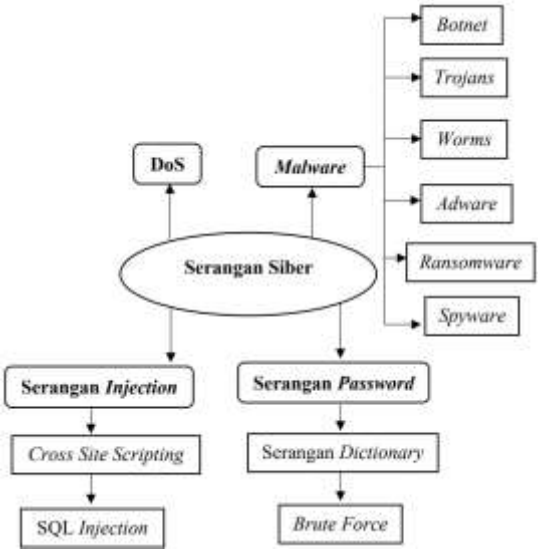
Gambar 4. Taksonomi klasifikasi serangan berdasarkan *dataset* KDD'99



Gambar 5. Taksonomi klasifikasi serangan berdasarkan *dataset* UNSW-NB15

Jenis serangan siber lainnya yang terdapat di *host* dan di setiap layer keamanan jaringan namun merupakan kategori serangan siber langka seperti yang disebutkan dalam penelitian (Bagui et al., 2019) yaitu *backdoor*, *shellcode*, dan *worms*. Serangan *backdoor* juga dijelaskan kembali dalam penelitian (Goldblum et al., 2023). Tipe-tipe umum serangan siber juga dijelaskan dalam penelitian (Ahmetoglu & Das, 2022), namun dalam penelitian ini tipe umum tersebut disaring kembali disesuaikan dengan yang terdapat *host* dan di setiap layer keamanan jaringan seperti yang ditunjukkan pada gambar 6.

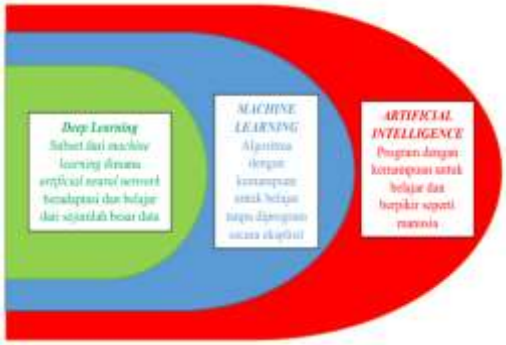
Terdapat 2 (dua) macam kategori serangan siber *internet of things* (IoT) yang dijelaskan dalam penelitian (Mohd Yusof & Sulaiman, 2022) yaitu serangan perangkat lunak dan serangan jaringan. Kemudian dalam penelitian ini, 2 (dua) kategori tersebut disaring kembali disesuaikan dengan yang terdapat *host* dan di setiap layer keamanan jaringan. Sehingga serangan perangkat lunak meliputi injeksi kode, *butter overflow, malware,* dan *side channel attack*. Sedangkan serangan jaringan meliputi *man in the middle,* DoS, DDoS, dan serangan RPL. Contoh serangan siber secara umum juga disebutkan kembali dalam penelitian (Barik et al., 2022) kemudian disaring hanya yang terdapat di *host* dan di setiap layer keamanan jaringan yaitu DoS, *user to root* (U2R), dan *remote to local* (R2L). Menurut penelitian (de Azambuja et al., 2023) serangan siber meliputi serangan aplikasi protokol, serangan terhadap ML dan analisis *data*, serangan injeksi, serangan *time delay, spoofing, ransomware,* DDos. Menurut (Dasgupta et al., 2022) serangan siber terbagi menjadi *root access compromise, web access compromise* yang meliputi SQL injeksi dan *cross site scripting,* kemudian *malware* meliputi virus, *worm,* trojan, *spyware,* dan *ransomware.* DoS meliputi *host*, jaringan, dan serangan terdistribusi



Gambar 6. Tipe-tipe umum serangan siber

2) Teknik atau metode apa saja yang ada dalam AI (*artificial intelligence*)? (*RQ* 2)

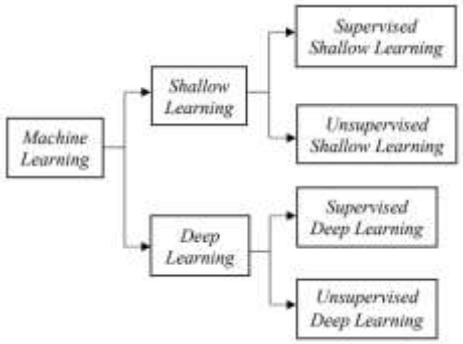
AI *(Artificial Intelligence), machine learning, dan deep learning* merupakan suatu hubungan yang tidak dapat dipisahkan. Ketiganya saling menyokong dan selalu berkaitan antara satu dan yang lainnya dalam implementasinya. Ilustrasi hubungan antara AI, *machine learning, dan deep learning* dapat dilihat pada gambar 7.



Gambar 7. Hubungan AI, *machine learning*, dan *deep learning*

Pandangan yang berbeda dan aplikasinya dapat menyebabkan klasifikasi yang berbeda terhadap *machine learning*. Oleh karena itu, tidak mungkin hanya merujuk sepenuhnya ke 1 (satu) literatur mengenai taksonomi *machine learning*. Seperti yang ditunjukkan pada gambar 8. dijelaskan dalam penelitian (Apruzzese et al., 2018), dimana taksonomi ini secara khusus berorientasi pada operator keamanan dan menghindari tujuan ambisius untuk menyajikan klasifikasi akhir yang dapat memuaskan semua pakar AI dan kasus aplikasi.

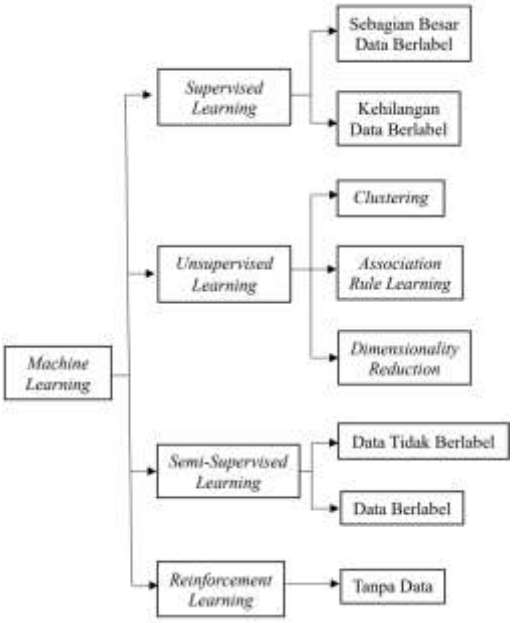
Pada gambar 8. algoritma ML tradisional yang saat ini dapat dirujuk sebagai *shallow learning* (SL), berlawanan dengan *deep learning* yang lebih baru. *Shallow learning* membutuhkan pakar domain yang dapat melakukan tugas penting untuk mengidentifikasi karakteristik *data* yang relevan sebelumnya untuk mengeksekusi algoritma SL. *Deep learning* mengandalkan representasi berlapis-lapis dari input *data* dan dapat melakukan pemilihan fitur secara mandiri melalui suatu proses pembelajaran representasi terdefinisi (Apruzzese et al., 2018).



Gambar 8. Klasifikasi *machine learning* untuk aplikasi keamanan siber

Dalam penelitian (Veiga, 2018) dikatakan bahwa hanya ML cabang AI yang berhasil diterapkan untuk memecahkan sebagian kecil dari masalah keamanan siber dan dijelaskan juga klasifikasi teknik ML terdiri dari *supervised* dan *unsupervised learning*. Kemudian dalam penelitian (Sen et al., 2022) teknik ML terbagi menjadi *supervised learning, unsupervised learning*, dan *semi supervised learning.* Selanjutnya, dalam (Saravanan & Sujatha, 2018) dijelaskan bahwa klasifikasi teknik ML terbagi menjadi *supervised learning, unsupervised learning, semi supervised learning,* dan *reinforcement learning.* Gambar 9. menunjukkan klasifikasi ML seperti yang dijelaskan dalam penelitian (Veiga, 2018), (Sen et al., 2022), dan (Saravanan & Sujatha, 2018).

Dalam penelitian (Sarker et al., 2020) lebih lengkap lagi dijelaskan bahwa teknik ML terbagi menjadi *supervised learning, unsupervised learning*, *neural network* dan *deep learning,* serta *semi supervised learning*. Dalam Penelitian (Apruzzese et al., 2023) tipe algoritma ML terdiri dari *supervised, unsupervised, shallow,* dan *deep learning.* Kemudian ML untuk deteksi ancaman terdiri dari pendekatan *suverpised* dan *unsupervised.*



Gambar 9. Tampilan parsial algoritma ML dan aplikasinya untuk keamanan siber

3) Teknik atau metode AI (*artificial intelligence*) apa saja yang biasanya digunakan untuk mengatasi masalah keamanan siber? (*RQ* 3)

Beberapa teknik atau metode AI (*artificial intelligence*) yang biasanya digunakan untuk mengatasi masalah keamanan siber menurut (Kumar et al., 2021) metode *Kmeans clustering* juga efektif mengatasi masalah keamanan siber. Dalam (Farooq & Otaibi, 2018) juga disebutkan kembali metode *K-means clustering, one class* SVM (OCSVM), regresi linear, dan *random forest* dapat digunakan untuk mengatasi masalah keamanan siber. *Decision tree, artificial neural networks (ANN), naïve bayes, support vector machine (SVM), algoritma genetik (GA), k-means clustering, k-nearest neighbor,* logika *fuzzy,* model *hidden markov, swarm intelligence,* dan *ensemble learning* adalah teknik yang digunakan dalam *machine learning* dijelaskan dalam penelitian (Mishra et al., 2019).

SVM*, decision tree, k-nearest neighbor, random forest, naïve bayes, recurrent neural network* (RNN)*, convolutional neural networks* (CNN)*, deep belief network* (DBN)*, auto encoder, dan reinforcement learning* dalam penelitian menurut (Shaukat et al., 2020) juga dapat digunakan untuk mengatasi masalah keamanan siber. CNN, SVM, ANN disebut juga oleh (Zhimin Zhang et al., 2021). Dalam penelitian (Laqtib et al., 2020) terdapat CNN, BLSTM, dan DBN. Selanjutnya, metode SVM , pengklasifikasian *K-nearest neighbor*, algoritma *decision tree*, DBN, RNN, dan CNN disebutkan dalam penelitian (Xin et al., 2018). *Naïve bayes classifier, decision tree (J48), k-means clustering* disebutkan dalam penelitian (Bagui et al., 2019).

Kemudian, metode *multi layer neural network, RNN, LSTM* disebutkan dalam penelitian (Larriva-Novo et al., 2020). Menurut (Barik et al., 2022) CNN, RNN, DNN juga dapat digunakan untuk mengatasi masalah keamanan siber. DBN, *naïve bayes*, algoritma C4.5, algoritma REPTree, SVM, algoritma genetik (GA), MLP, KNN, *random forest*, CNN, RNN juga disebutkan menurut (Abdullahi et al., 2022) dapat digunakan untuk mengatasi masalah keamanan siber. Teknik atau metode AI (*artificial intelligence*) yang biasanya digunakan untuk mengatasi masalah keamanan siber seperti yang telah disebutkan sebelumnya juga telah disebutkan kembali dalam penelitian (Bécue et al., 2021).

Kemudian dalam penelitian (Ahmetoglu & Das, 2022) dijelaskan juga berbagai teknik ML yaitu *deep learning, ensemble, regularization, rule system, bayesian, regression, dimensionality reduction, decision tree, instance based,* dan *clustering*. Sedangkan, penelitian (Yan et al., 2022) menjelaskan bahwa model ML terbagi menjadi 3 kategori yaitu model *linear,* model *tree,* dan model parametrik. Model *linear* meliputi *linear regression* dan SVM. Model *tree* meliputi *gradient boosting machine* (GBM), *extreme gradient boosting* (XGBoost), dan *natural gradient boosting* (NGBoost). Model parametrik adalah *generative additive model* (GAM). XGBoost juga dijelaskan dalam penelitian (Elsisi et al., 2021).

Dalam penelitian (Dasgupta et al., 2022) dijelaskan bahwa algoritma ML tradisional meliputi *decision tree,* SVM, *naïve bayes,* dan *K-means clustering.* Sedangkan algoritma *neural network* meliputi ANN, CNN, RNN, *restricted boltzmann machine,* dan DBN. Oleh (Waqas et al., 2022) menjelaskan SVM, *logistic regression*, *deep multilayer perception,* RNN, *semi supervised learning, reinforcement learning,* DQN teknik, *deep learning, self taught learning,* DBN. Oleh (Nguyen & Reddi, 2021) menjelaskan *deep reinforcement learning* (DRL), dan DQN. Oleh (de Azambuja et al., 2023) menjelaskan CNN, *deep autoencoders* (DAE), DBN, RNN, *generative adversarial network* (GAN), DRL. GAN juga disebutkan kembali dalam penelitian (Yinka-Banjo & Ugot, 2020). DNN dijelaskan dalam penelitian (Ibor et al., 2020) dan (Vinayakumar et al., 2019). K-*nearest neighbor, decision tree, random forest, neural networks,* SVM, GAN dijelaskan dalam penelitian (Mari et al., 2023). Kemudian, (Kaja et al., 2019) menjelaskan *Decision tree* (J48), *random forest, adaptive boosting, naïve bayes.* Dalam penelitian (Tian et al., 2020) juga dijelaskan DBN, RBM, dan CRBM.

4) *Dataset* apa yang banyak digunakan pada penelitian AI (*artificial intelligence*) terkait dengan keamanan siber? (*RQ* 4)

Dataset sangat penting untuk pelatihan dan pengujian model *machine learning* (ML). Ada tidaknya perwakilan maupun kumpulan *data* dapat menjadi tolak ukur untuk setiap *domain* ancaman siber (Shaukat et al., 2020). Dijelaskan bahwa terdapat beberapa *dataset* publik yang tersedia untuk berbagai macam kategori serangan siber, seperti dataset untuk *malware* yaitu N-BaIoT, IoTPOT, IoT-23, EMBER, Genome Project, VirusShare, CICAndMal2017, dan DREBIN. Kemudian dataset untuk *spam,* yaitu SMS *Spam* v.1, EnronSpam, dan ISCX-URL2016. Dataset untuk intrusi jaringan yaitu NSL-KDD, UNB ISCX 2012, AWID, CIC-IDS2017, CIC-DDoS2019, TON_IoT, LITNET-2020, ADFA-LD, dan UNSW-NB15. Dataset untuk DGA yaitu UMUDGA dan AmritaDGA. Dataset untuk DoS yaitu InSDN dan UNB ISCX 2012. Terakhir dataset untuk botnet yaitu CTU-13, CIC-IDS2017, ISOT Botnet Dataset, BOT-IoT dataset, dan Genome Project (Zhibo Zhang et al., 2022).

Dalam penelitian (Shaukat et al., 2020) disebutkan dataset DARPA 1999 dan 1998, KDD CUP 99, NSL-KDD, *Spambase,* DARPA 2000, *Enron,* SMS *spam collection*, ISoT, ADFA, CTU, *VirusShare, Android Validation, Enron*-2015, *Kharon*, ISCX-URL, CICIDS, CICandMal *Android*, Bot-IoT, CICandMaldroid. Kemudian, dataset NSL-KDD disebutkan menurut (Laqtib et al., 2020). Dataset DARPA 1998, KDD CUP 99, NSL-KDD, CIC IDS 2017, CSE-CIC-IDS2018, ADFA 2013, dan UNSW-NB15 juga disebutkan dalam penelitian (Yadav et al., 2020). Menurut (Xin et al., 2018) disebutkan *dataset* deteksi intrusi DARPA, *dataset* KDD CUP 99, *dataset* NSL-KDD, dan *dataset* ADFA.

Dataset UNSW-NB15 juga disebutkan dalam penelitian (Bagui et al., 2019) dan (Larriva-Novo et al., 2020). Menurut (Mohd Yusof & Sulaiman, 2022) *dataset* DARPA, KDD CUP 99, NSL-KDD CUP 99, CAIDA, CICDS 2017, ADFA-LD, ADFA-WD, *dataset* kyoto 2006+ juga dapat digunakan pada penelitian AI terkait dengan keamanan siber. Kemudian, *dataset* ECU-IoFT juga disebutkan dalam penelitian (Ahmed et al., 2022). *Dataset* yang banyak digunakan pada penelitian AI (*artificial intelligence*) terkait dengan keamanan siber seperti yang telah disebutkan sebelumnya juga telah disebutkan kembali dalam penelitian (Abdullahi et al., 2022) dan (Bécue et al., 2021). KDD99, UNSW-NB15, NSL-KDD, ISCX, ISOT *cloud intrusion,* HTTP CSIC, Kyoto 2006, CICIDS 2017, *industrial control system cyber attack dataset,* AWID, CSE-CIC-IDS2018, Bot-IoT, TON_IOT, InSDN dijelaskan dalam penelitian (Ferrag et al., 2022). DARPA, KDD'99 Cup, NSL-KDD, CAIDA, ISOT'10, ISCX'12, CTU-13, UNSW-NB15, CIC-IDS 2018 dan 2017, CIC-DDoS 2019, MAWI, ADFA IDS, CERT, *email*, DGA, *malware,* Bot-IoT juga dijelaskan dalam penelitian (Sarker et al., 2020).

MAWILab, *malware training set, dataset Los Alamos National Laboratory,* ICML-09, ADFA, *stratosphere lab dataset,* EMBER, *fake news, credbank,* PHEME, ISOT *fake news dataset, home* 2017 *fake news data, draper* VDISC *dataset*

dijelaskan dalam penelitian (Sen et al., 2022). KDD CUP 99, kyoto 2006+, NSL-KDD, ECML-PKDD 2007, *information security and object technology* (ISOT) *dataset,* HTTP CSIC 2010, *czech technical university* (CTU-13), ADFA, UNSW-NB15, UNB-CIC juga dijelaskan dalam penelitian (Dasgupta et al., 2022). *Dataset* yang telah disebutkan sebelumnya juga telah disebutkan kembali dalam penelitian (Ibor et al., 2020), (Mari et al., 2023), (Tian et al., 2020), dan (Vinayakumar et al., 2019) dengan tambahan *dataset* WSN-DS.

5) Teknik atau metode AI (*artificial intelligence*) mana yang secara spesifik tepat untuk menangani jenis serangan siber tertentu? (*RQ* 5)

Adanya kekhasan dari setiap ancaman siber yang menyulitkan, bahkan untuk model *machine learning* yang canggih ketika menghadapi serangan siber. Dalam penerapannya, tidak mungkin memberikan satu rekomendasi yang sama untuk semua serangan berdasarkan satu model *machine learning*. Berbagai kriteria seperti tingkat deteksi, kompleksitas waktu, klasifikasi waktu untuk mendeteksi serangan baru dan serangan *zero-day*, serta akurasi model *machine learning* (ML) seharusnya dipertimbangkan saat memilih model tertentu untuk mendeteksi sebuah serangan siber (Shaukat et al., 2020). Dalam penelitian (Mishra et al., 2019) menyebutkan kembali bahwa tidak semua intrusi dapat diatasi dengan satu teknik *machine learning* yang sama.

Tabel 3. Penggunaan Metode AI Berdasarkan Jenis Serangan Siber

Serangan	Metode	*Dataset*
Deteksi s*pam*	SVM, DBN, dan *clustering*	SMS *Spam* v.1, *EnronSpam*, dan ISCX-URL2016
Deteksi intrusi	ANN, SVM, dan *decision tree*	NSL-KDD, UNB ISCX 2012, AWID, CIC-IDS2017, CIC-DDoS2019, TON_IoT, LITNET-2020, ADFA-LD, dan UNSW-NB15
Deteksi *malware*	SVM dan *decision tree*	N-BaIoT, IoTPOT, IoT-23, EMBER, *Genome Project, VirusShare,* CIC&Mal2017, dan DREBIN
Akurasi deteksi	DBN+semi *supervised learning*	
Data rate analitik	*Clustering*	
Deteksi anomali	OCSVM	
Prediksi perilaku pengguna	Regresi linear	
Klasifikasi pesan	*Random forest*	
Deteksi serangan pada CPS	DNN	
Serangan siber langka	Seleksi fitur *hybrid* yaitu *k-means clustering*+seleksi subset Cfs, dan teknik klasifikasi yaitu *naïve bayes+decision tree* (J48)	UNSW-NB15
Probe	DBN, *naïve bayes,* C4.5, dan *REPTree*	
U2R	DBN, SVM, algoritma genetik, dan MLP	
R2L	DBN, KNN, algoritma genetik, dan *random forest*	
DoS	CNN, RNN, SVM, DBN, dan *random forest*	InSDN dan UNB ISCX 2012
Serangan aplikasi protokol, ML dan analisis data, injeksi, *time delay, spoofing, ransomware,* dan DDos	CNN, DAE, DBN, RNN, GAN, dan DRL	
Root/Web access compromise dan *malware*	*Decision tree,* SVM, *naïve bayes, K-means clustering,* ANN, CNN, RNN, *restricted boltzmann machine,* dan DBN	KDD CUP 99, kyoto 2006+, NSL-KDD, ECML-PKDD 2007, ISOT, HTTP CSIC 2010, CTU-13, ADFA, UNSW-NB15, UNB-CIC

Deteksi *spam* pada jaringan komputer dapat menggunakan teknik ML yaitu klasifikasi *support vector machine* (SVM), sedangkan jika menggunakan DL yaitu DBN *(Deep Belief Network)* dan teknik *clustering* (Shaukat et al., 2020). *Dataset* untuk *spam,* yaitu SMS *Spam* v.1, EnronSpam, dan ISCX-URL2016 (Zhibo Zhang et al., 2022). Deteksi intrusi pada jaringan komputer dapat menggunakan teknik ML yaitu *artificial neural networks* (ANN), SVM, dan *decision tree*. *Dataset* untuk intrusi jaringan yaitu NSL-KDD, UNB ISCX 2012, AWID, CIC-IDS2017, CIC-DDoS2019, TON_IoT, LITNET-2020, ADFA-LD, dan UNSW-NB15 (Zhibo Zhang et al., 2022). Deteksi *malware* pada jaringan komputer dapat menggunakan teknik ML yaitu SVM dan *decision tree,* kemudian untuk meningkatkan akurasi deteksinya dapat menggunakan DBN *(Deep Belief Network)* dikombinasikan dengan teknik semi *supervised learning* (Shaukat et al., 2020). *Dataset* untuk *malware* yaitu N-BaIoT, IoTPOT, IoT-23, EMBER, Genome Project, VirusShare, CICAndMal2017, dan DREBIN (Zhibo Zhang et al., 2022).

Data rate *analytic* dapat menggunakan algoritma *clustering*, deteksi anomali dalam proses eksekusi dapat menggunakan klasifikasi *one class* svm (ocsvm), memprediksi perilaku pengguna dapat menggunakan regresi linear, deteksi anomali dalam proses eksekusi dapat menggunakan klasifikasi *one class* svm (ocsvm), dan klasifikasi pesan dapat menggunakan *random forest* (Farooq & Otaibi, 2018). Untuk fase deteksi serangan pada *cyber physical systems* (CPS) dapat menggunakan struktur

deep neural network (Zarandi & Sharifi, 2020). Menangani kategori serangan siber langka seperti *backdoor*, *shellcode*, dan *worms* dapat menggunakan *dataset* UNSW-NB15 dengan metode seleksi fitur *hybrid* yaitu kombinasi *k-means clustering* dan seleksi subset Cfs serta 2 (dua) teknik klasifikasi yaitu *naïve bayes* dan *decision tree* (J48) (Bagui et al., 2019).

Namun dalam penelitian (Bagui et al., 2019) dijelaskan kembali hasilnya bahwa metode seleksi fitur *hybrid* dengan teknik *naïve bayes* mampu mengidentifikasi serangan siber langka, meningkatkan akurasi klasifikasi dan tingkar *false alarm* yang lebih rendah untuk sebagian besar serangan siber terutama serangan siber langka. Sedangkan teknik *decision tree* (J48) tidak bekerja lebih baik dengan metode seleksi fitur *hybrid* tersebut, tetapi tingkat klasifikasinya untuk semua kategori serangan sudah sangat tinggi, dengan atau tanpa pemilihan fitur. Dalam penelitian (Abdullahi et al., 2022) juga disebutkan metode AI yang digunakan berdasarkan kategori serangan seperti serangan *probe* dapat menggunakan teknik ML yaitu DBN, *naïve bayes,* algoritma C4.5, dan algoritma *REPTree.* Kemudian serangan U2R dapat menggunakan teknik ML yaitu DBN, SVM, algoritma genetik, dan MLP (Abdullahi et al., 2022). Serangan R2L dapat menggunakan teknik ML yaitu DBN, KNN, algoritma genetic, dan *random forest* (Abdullahi et al., 2022). Serangan DoS dapat menggunakan teknik ML yaitu CNN, RNN, SVM, DBN, dan *random forest* (Abdullahi et al., 2022). *Dataset* untuk DoS yaitu InSDN dan UNB ISCX 2012 (Zhibo Zhang et al., 2022).

Dalam penelitian (de Azambuja et al., 2023) menjelaskan bahwa serangan aplikasi protokol, serangan terhadap ML dan analisis *data*, serangan injeksi, serangan *time delay, spoofing, ransomware,* DDos dapat menggunakan teknik ML yaitu CNN, *deep autoencoders* (DAE), DBN, RNN, *generative adversarial network* (GAN), dan DRL. Terakhir, dalam penelitian (Dasgupta et al., 2022) juga dijelaskan bahwa serangan siber seperti *root access compromise, web access compromise, dan malware* juga dapat ditangani menggunakan algoritma ML tradisional meliputi *decision tree,* SVM, *naïve bayes,* dan *K-means clustering.* Kemudian, algoritma *neural network* meliputi ANN, CNN, RNN, *restricted boltzmann machine,* dan DBN. Dalam penelitian (Dasgupta et al., 2022) juga disebutkan untuk menangani serangan siber tersebut dapat menggunakan *dataset* KDD CUP 99, kyoto 2006+, NSL-KDD, ECML-PKDD 2007, *information security and object technology* (ISOT) *dataset,* HTTP CSIC 2010, *czech technical university* (CTU-13), ADFA, UNSW-NB15, dan UNB-CIC.

4. KESIMPULAN DAN SARAN

4.1. KESIMPULAN

Penelitian SLR ini melakukan survei pada 44 paper studi primer yang diterbitkan antara tahun 2018 hingga 2023. Dari *paper* tersebut diperoleh 30 *paper* membahas penggunaan teknik *machine learning* dan *deep learning,* 19 *paper* yang membahas penggunaan *dataset*, 13 *paper* membahas peluang penelitian masa depan, dan 5 *paper* membahas terkait *tools.*

Berdasarkan hasil survei ini diperoleh serangan *malware, spam,* intrusi jaringan, dan DoS adalah serangan yang paling banyak ditemukan di sistem *host* maupun di setiap lapisan keamanan jaringan. Selain itu, serangan siber langka yang juga ditemukan yaitu *backdoor*, *shellcode*, dan *worms.* Teknik AI yang dibahas pada penelitian keamanan siber terdiri dari *machine learning* dan *deep learning.* Teknik *machine learning* yang paling banyak digunakan untuk mengatasi masalah keamanan siber yaitu SVM (*support vector machine*), sementara teknik *deep learning* yaitu CNN (*convolutional neural networks*). *Dataset* yang paling banyak digunakan pada penelitian AI yaitu NSL-KDD dan KDD CUP'99. Dari hasil penelitian survei ini diperoleh pemetaan berbagai teknik atau metode AI yang secara spesifik tepat menangani jenis serangan siber tertentu. Hasil pemetaan ini diharapkan dapat menjadi landasan dalam membuka peluang-peluang penelitian baru dalam dunia keamanan siber.

Hal-hal yang masih menjadi tantangan dalam penelitian ini yaitu *tools* yang relevan dan terbukti memiliki kinerja baik dalam menerapkan metode AI masih sangat jarang ditemukan penelitiannya, Padahal, *tools* sangat penting berkaitan dengan alat bantu yang mendukung pekerjaan para peneliti dalam mengekstrak dan menerapkan metode AI yang terus berkembang. Hal ini menjadi perhatian lebih lanjut pada penelitian selanjutnya. Secara umum, hasil dari penelitian ini diharapkan dapat berkontribusi dalam memberikan wawasan baru di dunia keamanan siber untuk membuka peluang penelitian masa depan, terutama bagi para peneliti pemula yang ingin melakukan riset di bidang keamanan siber.

4.2. SARAN

Dalam penelitian ini telah disebutkan berbagai macam *dataset* yang banyak digunakan untuk mengatasi masalah keamanan siber dan sudah ada juga disebutkan beberapa *dataset* publik yang tersedia untuk beberapa macam kategori serangan siber. Diharapkan untuk penelitian selanjutnya dapat menganalisis kembali terkait penggunaan *dataset* yang secara spesifik tepat untuk menangani jenis serangan siber tertentu lengkap dengan teknik atau metode *machine learning* yang digunakan. Kemudian dari analisis tersebut diharapkan para peneliti keamanan siber dapat mengimplementasikannya dalam sebuah sistem sehingga dapat benar-benar mengukur tingkat keefektifannya.

DAFTAR PUSTAKA

ABDULLAHI, M., BAASHAR, Y., ALHUSSIAN, H., ALWADAIN, A., AZIZ, N., CAPRETZ, L. F., & ABDULKADIR, S. J., 2022. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. *Electronics (Switzerland)*, *11*(2), 1–27. https://doi.org/10.3390/electronics11020198

AHMED, M., COX, D., SIMPSON, B., & ALOUFI, A., 2022. ECU-IoFT: A Dataset for Analysing Cyber-Attacks on Internet of Flying Things. *Applied Sciences (Switzerland)*, *12*(4), 1–12. https://doi.org/10.3390/app12041990

AHMETOGLU, H., & DAS, R., 2022. A Comprehensive Review on Detection of Cyber-Attacks: Data sets, Methods, Challenges, and Future Research Directions. *Internet of Things (Netherlands)*, *20*, 1–25. https://doi.org/10.1016/j.iot.2022.100615

APRUZZESE, G., FERRETTI, L., MARCHETTI, M., COLAJANNI, M., & GUIDO, A., 2018. On The Effectiveness of Machine Learning and Deep Learning Algorithms for Cyber Security. *10th International Conference on Cyber Conflict*, 371–390. https://doi.org/10.1007/s11831-020-09478-2

APRUZZESE, G., LASKOV, P., MONTES DE OCA, E., MALLOULI, W., BRDALO RAPA, L., GRAMMATOPOULOS, A. V., & DI FRANCO, F., 2023. The Role of Machine Learning in Cybersecurity. *Digital Threats: Research and Practice*, *4*(1). https://doi.org/10.1145/3545574

BAGUI, S., KALAIMANNAN, E., BAGUI, S., NANDI, D., & PINTO, A., 2019. Using machine learning techniques to identify rare cyber-attacks on the UNSW-NB15 dataset. *Security and Privacy*, *2*(6). https://doi.org/10.1002/spy2.91

BARIK, K., MISRA, S., KONAR, K., FERNANDEZ-SANZ, L., & KOYUNCU, M., 2022. Cybersecurity Deep: Approaches, Attacks Dataset, and Comparative Study. *Applied Artificial Intelligence*, *36*(1). https://doi.org/10.1080/08839514.2022.2055399

BÉCUE, A., PRAÇA, I., & GAMA, J., 2021. Artificial Intelligence, Cyber-Threats and Industry 4.0: Challenges and Opportunities. *Artificial Intelligence Review*, *54*(5), 3849–3886. https://doi.org/10.1007/s10462-020-09942-2

DASGUPTA, D., AKHTAR, Z., & SEN, S., 2022. Machine Learning in Cyber Security: a Comprehensive Survey. *Journal of Defense Modeling and Simulation*, *19*(1), 57–106. https://doi.org/10.1177/1548512920951275

DE AZAMBUJA, A. J. G., PLESKER, C., SCHÜTZER, K., ANDERL, R., SCHLEICH, B., & ALMEIDA, V. R., 2023. Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. *Electronics (Switzerland)*, *12*(8), 1–18. https://doi.org/10.3390/electronics12081920

ELSISI, M., TRAN, M. Q., MAHMOUD, K., MANSOUR, DI. E. A., LEHTONEN, M., & DARWISH, M. M. F., 2021. Towards Secured Online Monitoring for Digitalized GIS against Cyber-Attacks Based on IoT and Machine Learning. *IEEE Access*, *9*, 78415–78427. https://doi.org/10.1109/ACCESS.2021.3083499

FAROOQ, H. M., & OTAIBI, N. M., 2018. Optimal Machine Learning Algorithms for Cyber Threat Detection. *Proceedings - 2018 UKSim-AMSS 20th International Conference on Modelling and Simulation*, 32–37. https://doi.org/10.1109/UKSim.2018.00018

FERRAG, M. A., SHU, L., FRIHA, O., & YANG, X., 2022. Cyber Security Intrusion Detection for Agriculture 4.0: Machine Learning-Based Solutions, Datasets, and Future Directions. *IEEE/CAA Journal of Automatica Sinica*, *9*(3), 407–436. https://doi.org/10.1109/JAS.2021.1004344

GOLDBLUM, M., TSIPRAS, D., XIE, C., CHEN, X., SCHWARZSCHILD, A., SONG, D., … GOLDSTEIN, T., 2023. Dataset Security for Machine Learning: Data Poisoning, Backdoor Attacks, and Defenses. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *45*(2), 1563–1580. https://doi.org/10.1109/TPAMI.2022.3162397

GOYAL, Y., & SHARMA, A., 2019. A Semantic Machine Learning Approach for Cyber Security Monitoring. *Proceedings of The 3rd International Conference on Computing Methodologies and Communication*, 439–442. https://doi.org/10.1109/ICCMC.2019.8819796

HE, S., SHI, X., HUANG, Y., CHEN, G., & TANG, H., 2022. Design of Information System Security Evaluation Management System based on Artificial Intelligence. *IEEE 2nd International Conference on Electronic Technology, Communication and Information*, 967–970. https://doi.org/10.1109/ICETCI55101.2022.9832131

IBOR, A. E., OLADEJI, F. A., OKUNOYE, O. B., & EKABUA, O. O., 2020. Conceptualisation

of Cyberattack Prediction with Deep Learning. *Cybersecurity*, *3*(1). https://doi.org/10.1186/s42400-020-00053-7

KAJA, N., SHAOUT, A., & MA, D., 2019. An Intelligent Intrusion Detection System. *Applied Intelligence*, *49*(9), 3235–3247. https://doi.org/10.1007/s10489-019-01436-1

KAUR, R., GABRIJELČIČ, D., & KLOBUČAR, T., 2023. Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions. *Information Fusion*, *97*(April). https://doi.org/10.1016/j.inffus.2023.101804

KUMAR, S., SINGH, B. P., & KUMAR, V., 2021. A Semantic Machine Learning Algorithm for Cyber Threat Detection and Monitoring Security. *Proceedings of The 3rd International Conference on Advances in Computing, Communication Control and Networking*, 1963–1967. https://doi.org/10.1109/ICAC3N53548.2021.9725596

LAQTIB, S., YASSINI, K. EL, & HASNAOUI, M. L., 2020. a Technical Review and Comparative Analysis of Machine Learning Techniques for Intrusion Detection Systems in MANET. *International Journal of Electrical and Computer Engineering*, *10*(3), 2701–2709. https://doi.org/10.11591/ijece.v10i3.pp2701-2709

LARRIVA-NOVO, X. A., VEGA-BARBAS, M., VILLAGRA, V. A., & SANZ RODRIGO, M., 2020. Evaluation of Cybersecurity Data Set Characteristics for Their Applicability to Neural Networks Algorithms Detecting Cybersecurity Anomalies. *IEEE Access*, *8*, 9005–9014. https://doi.org/10.1109/ACCESS.2019.2963407

MARI, A. G., ZINCA, D., & DOBROTA, V., 2023. Development of a Machine-Learning Intrusion Detection System and Testing of Its Performance Using a Generative Adversarial Network. *Sensors (Basel, Switzerland)*, *23*(3). https://doi.org/10.3390/s23031315

MISHRA, P., VARADHARAJAN, V., TUPAKULA, U., & PILLI, E. S., 2019. A Detailed Investigation and Analysis of Using Machine Learning Techniques for Intrusion Detection. *IEEE Communications Surveys and Tutorials*, *21*(1), 686–728. https://doi.org/10.1109/COMST.2018.2847722

MOHD YUSOF, N. N., & SULAIMAN, N. S., 2022. Cyber Attack Detection Dataset: A Review. *Journal of Physics: Conference Series*, *2319*(1), 1–6. https://doi.org/10.1088/1742-6596/2319/1/012029

NGUYEN, T. T., & REDDI, V. J., 2021. Deep Reinforcement Learning for Cyber Security. *IEEE Transactions on Neural Networks and Learning Systems*, *PP*, 1–17. https://doi.org/10.1109/TNNLS.2021.3121870

SAGAR, B. ., NIRANJAN, S., KASHYAP, N., & SACHIN, D., 2019. Providing Cyber Security Using Artificial Intelligence - A Survey. *Proceedings of The 3rd International Conference on Computing Methodologies and Communication*, 717–720. https://doi.org/10.1109/ICCMC.2019.8819719

SARAVANAN, R., & SUJATHA, P., 2018. A State of Art Techniques on Machine Learning Algorithms : A Perspective of Supervised Learning Approaches in Data Classification. *Second International Conference on Intelligent Computing and Control Systems (ICICCS)*, 945–949. Retrieved from https://ieeexplore.ieee.org/abstract/document/8663155

SARKER, I. H., KAYES, A. S. M., BADSHA, S., ALQAHTANI, H., WATTERS, P., & NG, A., 2020. Cyber Security Data Science: an Overview From Machine Learning Perspective. *Journal of Big Data*, *7*(1). https://doi.org/10.1186/s40537-020-00318-5

SEN, R., HEIM, G., & ZHU, Q., 2022. Artificial Intelligence and Machine Learning in Cybersecurity: Applications, Challenges, and Opportunities for MIS Academics. *Communications of the Association for Information Systems*, *51*(1), 179–209. https://doi.org/10.17705/1CAIS.05109

SHAUKAT, K., LUO, S., VARADHARAJAN, V., HAMEED, I. A., & XU, M., 2020. A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. *IEEE Access*, *8*, 222310–222354. https://doi.org/10.1109/ACCESS.2020.3041951

TIAN, Q., HAN, D., LI, K.-C., LIU, X., DUAN, L., & CASTIGLIONE, A., 2020. An Intrusion Detection Approach Based on Improved Deep Belief Network and LightGBM. *Applied Intelligence*, 40–44. https://doi.org/10.1109/ISCSIC57216.2022.00020

TRUONG, T. C., DIEP, Q. B., & ZELINKA, I., 2020. Artificial Intelligence in the Cyber Domain: Offense and Defense. *Symmetry*, *12*(3), 1–24. https://doi.org/10.3390/sym12030410

VEIGA, A. P., 2018. Applications of Artificial

Intelligence to Network Security. *ITEC 625-Information Systems Infrastructure*. Retrieved from http://arxiv.org/abs/1803.09992

VINAYAKUMAR, R., ALAZAB, M., SOMAN, K. P., POORNACHANDRAN, P., AL-NEMRAT, A., & VENKATRAMAN, S., 2019. Deep Learning Approach for Intelligent Intrusion Detection System. *IEEE Access*, *7*, 41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334

WAGUIE, F. T., & AL-TURJMAN, F., 2022. Artificial Intelligence for Edge Computing Security: A Survey. *International Conference on Artificial Intelligence in Everything (AIE)*, 446–450. https://doi.org/10.1109/aie57029.2022.00091

WAQAS, M., TU, S., HALIM, Z., REHMAN, S. U., ABBAS, G., & ABBAS, Z. H., 2022. The Role of Artificial Intelligence and Machine Learning in Wireless Networks Security: Principle, Practice and Challenges. In *Artificial Intelligence Review* (Vol. 55). https://doi.org/10.1007/s10462-022-10143-2

XIN, Y., KONG, L., LIU, Z., CHEN, Y., LI, Y., ZHU, H., … WANG, C., 2018. Machine Learning and Deep Learning Methods for Cybersecurity. *IEEE Access*, *6*, 35365–35381. https://doi.org/10.1109/ACCESS.2018.2836950

YADAV, R., PATHAK, P., & SARASWAT, S., 2020. Comparative Study of Datasets Used in Cyber Security Intrusion Detection. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *6*(5), 302–312. https://doi.org/10.32628/cseit2063103

YAN, F., WEN, S., NEPAL, S., PARIS, C., & XIANG, Y., 2022. Explainable Machine Learning in Cyber Security: A Survey. *International Journal of Intelligent Systems*, *37*(12), 12305–12334. https://doi.org/10.1002/int.23088

YINKA-BANJO, C., & UGOT, O. A., 2020. A Review of Generative Adversarial Networks and its Application in Cyber Security. *Artificial Intelligence Review*, *53*(3), 1721–1736. https://doi.org/10.1007/s10462-019-09717-4

ZARANDI, Z. N., & SHARIFI, I., 2020. Detection and Identification of Cyber-Attacks in Cyber-Physical Systems Based on Machine Learning Methods. *11th International Conference on Information and Knowledge Technology*, 107–112. https://doi.org/10.1109/IKT51791.2020.9345627

ZHANG, ZHIBO, HAMADI, H. AL, DAMIANI, E., YEUN, C. Y., & TAHER, F., 2022. Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. *IEEE Access*, *10*, 93104–93139. https://doi.org/10.1109/ACCESS.2022.3204051

ZHANG, ZHIMIN, NING, H., SHI, F., FARHA, F., XU, Y., XU, J., … CHOO, K. K. R., 2021. Artificial Intelligence in Cyber Security: Research Advances, Challenges, and Opportunities. *Artificial Intelligence Review*, *55*(2), 1029–1053. https://doi.org/10.1007/s10462-021-09976-0