Indonesian Journal of Electronics and Instrumentation Systems (IJEIS)
Vol.12, No.1, April 2022, pp. 37~46
ISSN (print): 2088-3714, ISSN (online): 2460-7681
DOI: 10.22146/ijeis.69022

Pembelajaran Mesin untuk Sistem Keamanan - Tinjauan Literatur

Nuruddin Wiranda*[1], Fal Sadikin[2], Wanvy Arifha Saputra[3]
[1]Program Studi Pendidikan Komputer, FKIP, ULM, Banjarmasin, Indonesia
[2]PJJ Teknik Informatika, Universitas Amikom Yogyakarta, Yogyakarta, Indonesia
[3]Politeknik Negeri Banjarmasin, Banjarmasin, Indonesia
e-mail: ***[1]nuruddin.wd@ulm.ac.id,** [2]fal.sadikin@fu-berlin.de, [3]wanvysaputra@poliban.ac.id

Abstrak

Sistem keamanan merupakan salah satu topik yang krusial pada era transformasi digital. Dalam penggunaan teknologi digital, sistem keamanan digunakan untuk menjamin kerahasiaan, integritas, dan ketersediaan data. Teknik pembelajaran mesin dapat diterapkan untuk menunjang kemampuan beradaptasi sistem dengan lingkungan, sehingga dapat melakukan pencegahan, dekteksi dan perbaikan. Mengingat pentingnya hal tersebut, maka perlu adanya kajian literatur untuk memetakan sejauh mana pembelajaran mesin sudah diterapkan pada sistem keamanan. Pada makalah ini disajikan rangkuman dari 31 makalah penelitian untuk menentukan teknik atau metode pembelajaran mesin apa yang paling menjanjikan untuk melakukan pencegahan, dekteksi dan perbaikan. Tahapan penelitian pada makalah ini terdiri dari 6 tahapan, yaitu : merumuskan pertanyaan penelitian, proses pencarian artikel, mendokumentasikan stategi pencarian, melakukan pemilihan studi, penilaian kualitas artikel, dan proses ektraksi data yang diperolah dari artikel. Berdasarkan hasil kajian, diperoleh hasil bahwa metode K-means paling menjanjikan untuk melakukan pencegahan, sedangkan untuk melakukan deteksi dapat menggunakan SVM, dan untuk perbaikan keamanan dapat menerapkan pembelajaran mesin menggunakan fitur berbasis NLP.

Kata kunci*—Pembelajaran Mesin, Sistem Keamanan, Tinjauan Pustaka*

Abstract

Security systems are one of the crucial topics in the era of digital transformation. In the use of digital technology, security systems are used to ensure the confidentiality, integrity, and availability of data. Machine learning techniques can be applied to support the system's adaptability to the environment, so that prevention, detection and recovery can be carried out. Given the importance of these things, it is necessary to review the literature to find out how machine learning is applied to security systems. This paper presents a summary of 31 research papers to determine what machine learning techniques or methods are the most promising for prevention, detection and recovery. The research stages in this paper consist of 6 stages, namely: formulating research questions, searching for articles, documenting search strategies, selecting studies, assessing article quality, and extracting data obtained from articles. Based on the results of the study, it was found that the K-means method was the most promising for prevention, while for detection, SVM could be used, and for security recovery, machine learning could be implemented using NLP-based features.

Keywords— *Machine Learning, Security System, Literature review*

1. PENDAHULUAN

Internet awalnya dikembangkan untuk jaringan pribadi yang menghubungkan pemerintah, militer, dan peneliti akademis. Dengan demikian, tidak banyak kebutuhan terkait penggunaan protokol yang aman, paket terenkripsi, dan server yang handal. Penciptaan *world wide web* (www) mengantarkan Internet ke era Internet komersial, sehingga sangat sulit

Received September 9th,2021; Revised January 4th, 2022; Accepted March 30th, 2022

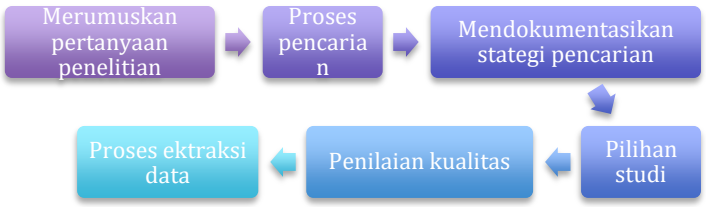
menerapkan mekanisme aman secara sempurna. Arsitek Internet tidak pernah menciptakan istilah seperti *spam*, *phishing*, *zombie*, dan *spyware* [1], tetapi istilah ini sekarang sering kita temukan.

Peran keamanan dalam penggunaan teknologi, kebijakan, dan pendidikan adalah untuk menjamin kerahasiaan, integritas, dan ketersediaan data selama proses penyimpanan, pemrosesan, dan transmisi. Secara umum, sistem keamanan dapat dilakukan melalui tiga hal yaitu pencegahan [2]–[4], pendeteksi [5]–[9], dan perbaikan [10], [11]. Di bidang kecerdasan buatan, keamanan data dapat dilakukan dengan memanfaatkan teknik-teknik pembelajaran mesin / *machine learning* (ML). Teknik ini dapat beradaptasi dengan cepat dengan lingkungan sehingga cocok untuk pencegahan, deteksi, dan perbaikan keamanan.

Tujuan utama dari penelitian ini adalah untuk melakukan tinjauan terkait pembelajaran mesin untuk sistem keamanan. Meskipun ada banyak studi penelitian tentang pembelajaran mesin untuk keamanan, sepengetahuan kami, hanya ada sedikit ulasan sistematis tentang topik ini. Pada makalah ini dikumpulkan dan dipilih dengan cermat sehubungan dengan pembelajaran mesin untuk sistem keamanan.

2. METODE PENELITIAN

Studi ini mengadopsi dan menggabungkan metode yang telah digunakan oleh Kitchenham dkk. [12] dan Liao dkk. [13]. Terdapat enam tahapan yang dilakukan dalam penelitian ini, seperti yang disajikan Gambar 1.



Gambar 1 Metode Penelitian

2.1 Merumuskan Pertanyaan Penelitian

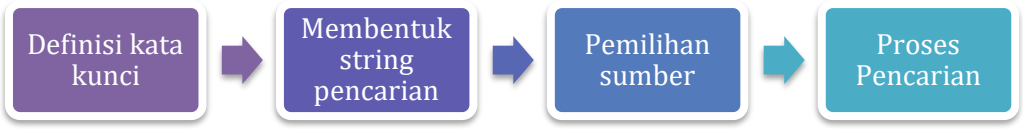
Tujuan utama dari tinjauan literatur sistematis ini adalah untuk menentukan pertanyaan yang dapat dicakup oleh pembelajaran mesin untuk keamanan dan keamanan untuk pembelajaran mesin, dan memberikan jawaban konkret untuk pertanyaan-pertanyaan ini. Research Question (RQ) untuk menjaga fokus review. Rincian deskriptif dan motivasi tentang pertanyaan-pertanyaan dalam penelitian ini tercantum pada Tabel 1.

Tabel 1 Motivasi Penelitian

Pertanyaan Penelitian (QR)	Motivasi
RQ1. Apa permasalahan, dalam implementasi pembelajaran mesin pada sistem keamanan?	Pertanyaan ini berfokus untuk mengetahui permasalahan saat mengimplementasikan pembelajaran mesin untuk sistem keamanan.
RQ2. Apa metode implementasi pembelajaran mesin pada sistem keamanan?	Pertanyaan ini berfokus untuk mengetahui metode dalam mengimplementasikan pembelajaran mesin untuk sistem keamanan.
RQ3. Apa tantangan dalam implementasi pembelajaran mesin pada sistem keamanan?	Pertanyaan ini berfokus untuk mengetahui tantangan saat mengimplementasikan pembelajaran mesin untuk sistem keamanan.
QR4. Metode apa yang paling menjanjikan untuk melakukan pencegahan, deteksi dan perbaikan sistem?	Pertanyaan ini berfokus untuk mengetahui metode apa yang paling menjanjikan untuk melakukan pencegahan, pendeteksian dan perbaikan sistem.

2.2 Proses Pencarian

Terdapat empat tahapan pada proses pencarian seperti pada Gambar 2, yaitu mendefinisikan kata kunci, membentuk string pencarian, pemilihan sumber artikel jurnal yang akan digunakan, dan melakukan proses pencarian artikel.



Gambar 2 Proses Pencarian Artikel Sumber

a) **Definisi kata kunci.** Kata kunci digunakan ke kueri pencarian untuk menemukan hasil pencarian yang paling relevan. Daftar berbagai kata kunci yang dibuat untuk tujuan pencarian disajikan pada Tabel 2.

Tabel 2 Kata Kunci untuk Pertanyaan Penelitian

Pertanyaan penelitian (*RQ*)	Kata kunci
RQ1. Apa permasalahan, dalam implementasi pembelajaran mesin pada sistem keamanan?	"Machine Learning *" OR "Machine Learning Problems*" AND "for Security *" *" OR "System".
RQ2. Apa metode implementasi pembelajaran mesin pada sistem keamanan?	"Machine Learning *" OR "Machine Learning Methods*" AND "for Security *".
RQ3. Apa tantangan dalam implementasi pembelajaran mesin pada sistem keamanan?	"Machine Learning *" OR "Machine Learning Difficulties" OR Machine Learning Challenges" AND "for Security *".
QR4. Metode apa yang paling menjanjikan untuk melakukan pencegahan, deteksi dan perbaikan sistem?	"Machine Learning *" OR "Machine Learning Difficulties" OR Machine Learning Challenges" AND "for Prevention *" OR "Detection" OR "Recovery".

b) **Membentuk String Pencarian**. String pencarian dibentuk berdasarkan kata kunci untuk setiap pertanyaan. String ini divalidasi oleh para ahli di bidang pembelajaran mesin dan sistem keamanan. String pencarian diperiksa terhadap sumber pencarian dan dimodifikasi hingga hasil terbaik relevan.

c) **Pemilihan Sumber.** Artikel yang dijadikan sumber adalah artikel yang terbit pada IEEE Xplore dan Science Direct.

d) **Proses Pencarian**. Pencarian dilakukan pada bulan April 2020 untuk menemukan studi kunci yang relevan dengan cara pencarian manual maupun otomatis.

2.3 Pemilihan Studi

Pada langkah ini, dokumen disiapkan yang berisi semua detail tentang strategi pencarian kami. Daftar makalah yang disertakan dan tidak disertakan juga didokumentasikan dan rinciannya ditunjukkan pada Tabel 3. Artikel yang disertakan dan tidak disertakan ditentukan berdasarkan kriteria pada Tabel 4.

Tabel 3 Sumber Data Online

Pengindeks Jurnal	Disertakan	Tidak disertakan	Jumlah
Science Direct	15	161	176
IEEE Xplore	16	61	77

Tabel 4 Kriteria Artikel yang Digunakan dan Tidak Digunakan

Kriteria artikel yang digunakan	Kriteria artikel yang tidak digunakan
• Makalah penelitian diterbitkan menggunakan bahasa Inggris; • Studi utama yaitu makalah penelitian asli; • Makalah penelitian yang relevan dengan topik utama; • Makalah penelitian mulai dari 2011 hingga 2020	• Makalah yang ditulis selain bahasa Inggris; • Makalah tidak menjawab pertanyaan penelitian atau tidak mendefinisikant topik dengan benar; • Penghapusan artikel duplikat; • Makalah penelitian dengan kurang dari tiga halaman

2.4 Penilaian Kualitas

Penilaian kualitas diterapkan setelah memilih artikel. Fokus dari proses ini adalah untuk meningkatkan kriteria seleksi untuk makalah yang akan dirangkum. Daftar pertanyaan *Quality Assessment* (QA) disusun berdasarkan penelitian Kitchenham and Charters [14]. Setiap makalah diperiksa untuk memilih studi yang lebih relevan sehingga sebagian besar akan memberikan jawaban atas RQ penelitian kami. Daftar pertanyaan penilaian kualitas tercantum pada Tabel 5. Setiap pertanyaan hanya memiliki tiga kemungkinan jawaban, yaitu "Ya" = 1, "Tidak" = 0 dan "Sebagian" = 0,5. Dalam penilaian kualitas, hanya skor di atas 66 yang diambil.

Tabel 5 Kriteria Artikel yang digunakan dan tidak

No	Pertanyaan
1	Apakah tujuan penelitian dinyatakan dengan jelas?
2	Apakah ada pembelajaran mesin untuk sistem keamanan yang disajikan?
3	Apakah ada solusi yang disediakan untuk RQ yang dirumuskan?
4	Apakah itu menjawab pembelajaran mesin untuk keamanan sistem?
5	Apakah teknik pembelajaran mesin terkait sistem keamanan berkontribusi pada penelitian ini?

2.5 Proses Ekstraksi Data

Ekstraksi dan klasifikasi data dilakukan secara bersamaan menggunakan prosedur yang dijelaskan di atas. Berikut data yang diperoleh dari setiap artikel: nomor makalah, masalah makalah, metode makalah, tantangan makalah, tahun dalam domain RQ1, RQ2, RQ3, dan QR4.

3. HASIL DAN PEMBAHASAN

Serangan yang paling sering dibahas pada sistem keamanan adalah *Injection* [15], DoS, Zombie, *Phishing*, *Man-in-the Middle* [16], *malware, eavesdropping, jamming, distributed denial of service* , *intrusi* dan *spoofing* [17]. Secara umum, sistem keamanan dapat dilakukan melalui tiga hal yaitu pencegahan [2]–[4], pendeteksi [5]–[9], [18], dan perbaikan [10], [11]. Pencegahan dapat dilakukan menggunakan SCADA, PLC, OpenPLC, Encryption, AES, K-Means, IPS, dan Mobile crowdsensing. Pendeteksian serangan dapat dilakukan dengan menggunakan teknik pembelajaran mesin.

Pembelajaran mesin juga dapat digunakan untuk perbaikan. Adapun metode yang bisa digunakan adalah Sparse Bayesian learning [10], Bayesian Principal Component Analysis(BPCA)[46], Decision Trees[47], Naive Bayes classifiers[47], and Natural language Processing (NLP) [11]. Pada Tabel 6, kami menyajikan ringkasan deskripsi masalah, metode, dan tantangan yang digunakan oleh beberapa penulis dalam literatur terbaru.

Terdapat sebanyak 40 macam teknik pembelajaran mesin yang dapat digunakan, diantaranya sebagai berikut : SVM[19][20], Random Forest(RF) [19], [21], KNN[22], [23], Decision Tree(DT)[19], BNN[24], Linear Regression(LR) [25][26], Linear Means Classifier(LMC)[27], Neural Network (NN) [20], one class SVM [28], K-means [29], Naive Bayes[30], Kernel Linear[31], Fisher linear discriminant (FLD)[32], Bayesnet[17], SVM Linear [33], Cloud Confidence DDOS Filtering (C2DF)[34], RNN[35], Regresi Polinomial (PR)[17], PDLM[16], RNN[35], DNN[36], Fuzzy C-means[9], C4.5[23], LS-SVM[21], CKNN[16], FCM-ANN[37], Logistic Regression (LR) [38], XGBoost classifier [39] [40], CNN[41], DNN[42], TSE[42], J48[19], [43], OneR[43], FFDNN [44], Mesin Boltzmann Terbatas [44], Deep auto-encoder [44], Deep migration learning [44], Self-Taught Learning [44], ReNN (Replicator Neural Network) [44] dan LSTM[40], [45].

Tabel 6 Ringkasan Survei Literatur

Ref. No	Permasalahan	Metode	Tantangan	Tahun	Publisher	Aktivitas keamanan
[2]	Menanamkan Enkripsi dan Sistem Pencegahan Intrusi Pembelajaran Mesin	SCADA, PLC, OpenPLC, Encryption, AES, K-Means, IPS	Menanamkan Enkripsi dan Sistem Pencegahan Intrusi Pembelajaran Mesin	2018	IEEE	Pencegahan
[3]	Pencegahan injeksi tugas tidak sah berorientasi baterai di *crowdsensing* seluler	Mobile crowdsensing	Pencegahan injeksi tugas tidak sah berorientasi baterai di crowdsensing seluler	2019	IEEE	Pencegahan
[25]	Cyber Threat Detection	OCSVM, LR, RF	Deteksi Ancaman Siber	2018	IEEE	Deteksi
[33]	Deteksi malware	SVM	Mengidentifikasi keluarga malware yang tidak dikenal yang bertanggung jawab atas kategori serangan Zero-Day DDoS.	2019	IEEE	Deteksi
[26]	Deteksi Serangan Phishing	LR, ANN	*Phishing*	2019	IEEE	Deteksi
[28]	Deteksi DoS Attack	PSD Based Entropy, SVM	*Intrusion detection system*	2019	IEEE	Deteksi
[19]	Deteksi penyusupan	KDD-CUP 99 and NSL-KDD	*Intrusion detection system*	2019	IEEE	Deteksi
[39]	Deteksi penyusupan	BSO, XGBoost, RF	Mendeteksi aktivitas berbahaya dalam jaringan VBM2M-C	2020	IEEE	Deteksi
[42]	Deteksi penyusupan	DT, RF, NB, DNN, etc	meminimalkan ukuran jenis serangan milik setiap partisi.	2021	IEEE	Deteksi
[40]	Deteksi penyusupan	NSL-KDD and CSE-CIC-IDS2018 , RF, SVM, XGBoost, LSTM, etc.	Membandingkan 24 metode pembelajaran mesin	2021	IEEE	Deteksi
[20]	Deteksi penyusupan	Dataset : KDDCup99, NSL-KDD, Kyoto 2006+. Algo: SVM	Membangun model yang dapat membedakan antara aktivitas normal dan anomali	2018	IEEE	Deteksi
[48]	Mendeteksi anomali dalam sistem IoT	ANN	Heterogenitas dalam sistem serta jumlah perangkat yang perlu ditangani.	2016	IEEE	Deteksi
[38]	Mendeteksi anomali	Lasso, LR, SVM, DT, AB, GF, FCNN.	Mendeteksi korelasi sinyal dan menggunakannya untuk deteksi anomali	2018	IEEE	Deteksi
[43]	Deteksi penyusupan	Dataset: CSIC 2010 HTTP; Algo: J48, NB, OneR	Kinerja algoritma pembelajaran mesin dalam deteksi serangan	2020	IEEE	Deteksi
[49]	Deteksi penyusupan	DARPA, UNM, Creech & Hu, KDD, ADFA-LD	mengevaluasi IDS berbasis data	2015	SD	Deteksi
[50]	Deteksi penyusupan	Markov decision process;	Pembelajaran perbedaan temporal tingkat lanjut untuk IDS	2015	SD	Deteksi

Ref. No	Permasalahan	Metode	Tantangan	Tahun	Publisher	Aktivitas keamanan
[51]	Deteksi perilaku malware	SVM	Deteksi perilaku malware dan pengembangan vaksin	2015	SD	Deteksi
[52]	Deteksi penyusupan	Ensemble; Genetic algorithm;	IDS menggunakan *Bagging*	2015	SD	Deteksi
[53]	Deteksi anomali	triggering relation discovery (TRD), NB, BN, SVM	Mendeteksi pola malware baru	2016	SD	Deteksi
[29]	Deteksi penyusupan	K-means, SVM	Mengklasifikasikan data jaringan ke dalam perilaku normal dan abnormal.	2017	SD	Deteksi
[54]	Deteksi Spam	fuzzy-based oversampling method	mengklasifikasikan spam Twitter	2017	SD	Deteksi
[55]	Masalah privasi pembelajaran mendalam kolaboratif dalam komputasi awan	Cryptography Machine learning Fully homomorphic encryption,	data dienkripsi dengan kunci yang berbeda, semua operasi termasuk hasil menengah harus aman.	2017	SD	Deteksi
[56]	Mendeteksi manipulasi pasar	KNN,DTC,LDA, QDA,ANN,LGR, SVM	menggunakan klasifikasi mendeteksi anomali	2017	SD	Deteksi
[57]	Mendeteksi Steganografi Jaringan Berbasis Penyimpanan	Random Forest algorithms Regarding	menciptakan ide dan metode inovatif untuk perlindungan menyembunyikan dan mentransmisikan informasi rahasia	2019	SD	Deteksi
[58]	Filter spam	SVM, NB, NN	pemfilteran spam email	2019	SD	Deteksi
[21]	Pendekatan IDS berbasis ML	MCLPDR, OS-ELM, SVM, RF, LS-SVM,	*state-of-the-art literature on ML*	2019	SD	Deteksi
[59]	Keamanan IoT	ML, AI	Masalah keamanan utama CIA, dan masalah lapisan-bijaksana diidentifikasi	2020	SD	Deteksi
[44]	Deteksi intrusi keamanan cyber	FFDNN, CNN, DNN, RNN, DBN, RBM , etc.	Survei pendekatan pembelajaran mendalam untuk deteksi intrusi keamanan cyber, kumpulan data yang digunakan, dan studi komparatif	2021	SD	Deteksi
[60]	Peningkatan Serangan Layanan	SVM	Peningkatan Serangan Layanan pada Jaringan Sensor Nirkabel Berbasis ML	2021	SD	Deteksi
[10]	Pola-coupled jarang bayesian belajar untuk pemulihan *block-sparse signals*	Sparse Bayesian learning	Pemulihan sinyal block-sparse	2015	IEEE	Perbaikan
[11]	Mengidentifikasi ekspektasi individu	SVM, LR, DT, MLP, NB,NLP	Mengidentifikasi harapan individu dalam pemulihan layanan	2019	IEEE	Perbaikan

4. KESIMPULAN

Kami melakukan tinjauan literatur untuk menganalisis ML untuk keamanan dan keamanan untuk ML. Tinjauan tersebut menyelidiki studi relevan yang menjawab tiga RQ. Secara keseluruhan, kami memperoleh 31 makalah penelitian setelah menerapkan kriteria seleksi kami. Berdasarkan hasil survey literature diketahui bahwa terdapat tiga area keamanan yaitu pencegahan, deteksi, dan pemulihan. Serangan yang umumnya dibahas yaitu Injection, *DoS attack, Zombie attack, Phishing attack, Man-in-the Middle attack, jamming, eavesdropping, distributed denial of service, malware, intrusion* dan *spoofing*. Adapun metode yang paling menjanjikan untuk melakukan pencegahan adalah K-means, sedangkan untuk melakukan deteksi dapat menggunakan SVM, dan untuk perbaikan keamanan dapat menerapkan pembelajaran mesin menggunakan fitur berbasis NLP.

UCAPAN TERIMA KASIH

Pekerjaan ini sebagian didukung oleh TIM Pendidikan Komputer FKIP Universitas Lambung Mangkurat, PJJ Teknik Informatika Universitas Amikom Yogyakarta, dan Politeknik Negeri Banjarmasin.

DAFTAR PUSTAKA

[1] M. A. . Maloof and J. Lakhmi, *Machine Learning and Data Mining for Comp Sec*. .

[2] T. Alves, R. Das, and T. Morris, "Embedding Encryption and Machine Learning Intrusion Prevention Systems on Programmable Logic Controllers," *IEEE Embed. Syst. Lett.*, vol. 10, no. 3, pp. 99–102, 2018, doi: 10.1109/LES.2018.2823906.

[3] Y. Zhang, M. Simsek, and B. Kantarci, "Machine learning-based prevention of battery-oriented illegitimate task injection in mobile crowdsensing," *WiseML 2019 - Proc. 2019 ACM Work. Wirel. Secur. Mach. Learn.*, pp. 31–36, 2019, doi: 10.1145/3324921.3328786.

[4] S. Das and M. J. Nene, "A survey on types of machine learning techniques in intrusion prevention systems," *Proc. 2017 Int. Conf. Wirel. Commun. Signal Process. Networking, WiSPNET 2017*, vol. 2018-Janua, pp. 2296–2299, 2018, doi: 10.1109/WiSPNET.2017.8300169.

[5] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016, doi: 10.1109/COMST.2015.2494502.

[6] R. Geetha and T. Thilagam, "A Review on the Effectiveness of Machine Learning and Deep Learning Algorithms for Cyber Security," *Arch. Comput. Methods Eng.*, pp. 371–390, 2020, doi: 10.1007/s11831-020-09478-2.

[7] L. Chen, S. Hou, and Y. Ye, "Securedroid: Enhancing security of machine learning-based detection against adversarial android malware attacks," *ACM Int. Conf. Proceeding Ser.*, vol. Part F1325, pp. 362–372, 2017, doi: 10.1145/3134600.3134636.

[8] I. H. Sarker, Y. B. Abushark, F. Alsolami, and A. I. Khan, "IntruDTree: A machine learning based cyber security intrusion detection model," *Symmetry (Basel).*, vol. 12, no. 5, pp. 1–15, 2020, doi: 10.3390/SYM12050754.

[9] F. Sadikin, T. van Deursen, and S. Kumar, "A ZigBee Intrusion Detection System for IoT using Secure and Efficient Data Collection," *Internet of Things*, vol. 12, p. 100306, 2020, doi: 10.1016/j.iot.2020.100306.

[10] J. Fang, Y. Shen, H. Li, and P. Wang, "Pattern-coupled sparse bayesian learning for recovery of block-sparse signals," *IEEE Trans. Signal Process.*, vol. 63, no. 2, pp. 360–372, 2015, doi: 10.1109/TSP.2014.2375133.

[11] Y. Liu, Y. Wan, and X. Su, "Identifying individual expectations in service recovery through natural language processing and machine learning," *Expert Syst. Appl.*, vol. 131, pp. 288–298, 2019, doi: 10.1016/j.eswa.2019.04.063.

[12] B. Kitchenham *et al.*,"Systematic literature reviews in software engineering-A tertiary study,"Inf.Softw.Technol,vol.52,no.8,pp.792–805,2010,doi:10.1016/j.infsof.2010.03.006

[13] B. Liao, Y. Ali, S. Nazir, L. He, and H. U. Khan, "Security Analysis of IoT Devices by Using Mobile Computing: A Systematic Literature Review," *IEEE Access*, vol. 8, pp. 120331–120350, 2020, doi: 10.1109/ACCESS.2020.3006358.

[14] B. Kitchenham and S. Charters, "Guidelines for performing Systematic Literature Reviews in Software Engineering," 2007, doi: 10.1145/1134285.1134500.

[15] M. Bagaa, T. Taleb, J. B. Bernabe, and A. Skarmeta, "A Machine Learning Security Framework for Iot Systems," *IEEE Access*, vol. 8, pp. 114066–114077, 2020, doi: 10.1109/ACCESS.2020.2996214.

[16] A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani, and F. M. Dakalbab, "Machine Learning for Cloud Security: A Systematic Review," *IEEE Access*, vol. 9, pp. 20717–20735, 2021, doi: 10.1109/ACCESS.2021.3054129.

[17] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp. 1686–1721, 2020, doi: 10.1109/COMST.2020.2986444.

[18] F. Liang, W. G. Hatcher, W. Liao, W. Gao, and W. Yu, "Machine Learning for Security and the Internet of Things: The Good, the Bad, and the Ugly," *IEEE Access*, vol. 7, pp. 158126–158147, 2019, doi: 10.1109/ACCESS.2019.2948912.

[19] S. Zwane, P. Tarwireyi, and M. Adigun, "Performance analysis of machine learning classifiers for intrusion detection," *2018 Int. Conf. Intell. Innov. Comput. Appl. ICONIC 2018*, pp. 1–5, 2019, doi: 10.1109/ICONIC.2018.8601203.

[20] A. G. Gedam and S. G. Shikalpure, "Direct kernel method for machine learning with support vector machine," *2017 Int. Conf. Intell. Comput. Instrum. Control Technol. ICICICT 2017*, vol. 2018-Janua, pp. 1772–1775, 2018, doi: 10.1109/ICICICT1.2017.8342839.

[21] K. A. P. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," *Comput. Networks*, vol. 151, pp. 147–157, 2019, doi: 10.1016/j.comnet.2019.01.023.

[22] E. Eziama, L. M. S. Jaimes, A. James, K. S. Nwizege, A. Balador, and K. Tepe, "Machine learning-based recommendation trust model for machine-to-machine communication," *2018 IEEE Int. Symp. Signal Process. Inf. Technol. ISSPIT 2018*, vol. 2019-Janua, pp. 1–6, 2018, doi: 10.1109/ISSPIT.2018.8705147.

[23] D. Kim, D. Shin, and D. Shin, "Unauthorized Access Point Detection Using Machine Learning Algorithms for Information Protection," *Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018*, pp. 1876–1878, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00284.

[24] E. Eziama, K. Tepe, A. Balador, K. S. Nwizege, and L. M. S. Jaimes, "Malicious Node Detection in Vehicular Ad-Hoc Network Using Machine Learning and Deep Learning," *2018 IEEE Globecom Work. GC Wkshps 2018 - Proc.*, pp. 1–6, 2019, doi: 10.1109/GLOCOMW.2018.8644127.

[25] H. M. Farooq and N. M. Otaibi, "Optimal machine learning algorithms for cyber threat detection," *Proc. - 2018 UKSim-AMSS 20th Int. Conf. Model. Simulation, UKSim 2018*, pp. 32–37, 2018, doi: 10.1109/UKSim.2018.00018.

[26] I. Ortiz Garces, M. F. Cazares, and R. O. Andrade, "Detection of phishing attacks with machine learning techniques in cognitive security architecture," *Proc. - 6th Annu. Conf. Comput. Sci. Comput. Intell. CSCI 2019*, pp. 366–370, 2019, doi: 10.1109/CSCI49370.2019.00071.

[27] M. Nassar, "A Practical Scheme for Two-Party Private Linear Least Squares," 2019, [Online]. Available: http://arxiv.org/abs/1901.09281.

[28] N. Zhang, F. Jaafar, and Y. Malik, "Low-Rate DoS Attack Detection Using PSD Based Entropy and Machine Learning," *Proc. - 6th IEEE Int. Conf. Cyber Secur. Cloud Comput. CSCloud 2019 5th IEEE Int. Conf. Edge Comput. Scalable Cloud, EdgeCom 2019*, pp.

59–62, 2019, doi: 10.1109/CSCloud/EdgeCom.2019.00020.

[29] W. L. Al-Yaseen, Z. A. Othman, and M. Z. A. Nazri, "Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system," *Expert Syst. Appl.*, vol. 67, pp. 296–303, 2017, doi: 10.1016/j.eswa.2016.09.041.

[30] K. Goeschel, "Reducing false positives in intrusion detection systems using data-mining techniques utilizing support vector machines, decision trees, and naive Bayes for off-line analysis," *Conf. Proc. - IEEE SOUTHEASTCON*, vol. 2016-July, 2016, doi: 10.1109/SECON.2016.7506774.

[31] K. Sharma and R. Nandal, "A literature study on machine learning fusion with IoT," *Proc. Int. Conf. Trends Electron. Informatics, ICOEI 2019*, vol. 2019-April, no. Icoei, pp. 1440–1445, 2019, doi: 10.1109/icoei.2019.8862656.

[32] C. A. Jensen, M. A. El-Sharkawi, and R. J. Marks, "Power system security assessment using neural networks: Feature selection using fisher discrimination," *IEEE Trans. Power Syst.*, vol. 16, no. 4, pp. 757–763, 2001, doi: 10.1109/59.962423.

[33] R. Vishwakarma and A. K. Jain, "A honeypot with machine learning based detection framework for defending IoT based botnet DDoS attacks," *Proc. Int. Conf. Trends Electron. Informatics, ICOEI 2019*, no. Icoei, pp. 1019–1024, 2019, doi: 10.1109/ICOEI.2019.8862720.

[34] W. Dou, Q. Chen, and J. Chen, "A confidence-based filtering method for DDoS attack defense in cloud environment," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1838–1850, 2013, doi: 10.1016/j.future.2012.12.011.

[35] P. Bahad, P. Saxena, and R. Kamal, "Fake News Detection using Bi-directional LSTM-Recurrent Neural Network," *Procedia Comput. Sci.*, vol. 165, no. 2019, pp. 74–82, 2019, doi: 10.1016/j.procs.2020.01.072.

[36] Y. Li, K. Xiong, T. Chin, and C. Hu, "A Machine Learning Framework for Domain Generation Algorithm-Based Malware Detection," *IEEE Access*, vol. 7, pp. 32765–32782, 2019, doi: 10.1109/ACCESS.2019.2891588.

[37] N. Pandeeswari and G. Kumar, "Anomaly Detection System in Cloud Environment Using Fuzzy Clustering Based ANN," *Mob. Networks Appl.*, vol. 21, no. 3, pp. 494–505, 2016, doi: 10.1007/s11036-015-0644-x.

[38] A. N. Sokolov, I. A. Pyatnitsky, and S. K. Alabugin, "Research of Classical Machine Learning Methods and Deep Learning Models Effectiveness in Detecting Anomalies of Industrial Control System," *Proc. - 2018 Glob. Smart Ind. Conf. GloSIC 2018*, pp. 1–6, 2018, doi: 10.1109/GloSIC.2018.8570073.

[39] E. Eziama, S. Ahmed, S. Ahmed, F. Awin, and K. Tepe, "Detection of Adversary Nodes in Machine-To-Machine Communication Using Machine Learning Based Trust Model," *2019 IEEE 19th Int. Symp. Signal Process. Inf. Technol. ISSPIT 2019*, 2019, doi: 10.1109/ISSPIT47144.2019.9001743.

[40] L. Liu, P. Wang, J. Lin, and L. Liu, "Intrusion Detection of Imbalanced Network Traffic Based on Machine Learning and Deep Learning," *IEEE Access*, vol. 9, pp. 7550–7563, 2021, doi: 10.1109/ACCESS.2020.3048198.

[41] F. O. Olowononi, D. B. Rawat, and C. Liu, "Resilient Machine Learning for Networked Cyber Physical Systems: A Survey for Machine Learning Security to Securing Machine Learning for CPS," *IEEE Commun. Surv. Tutorials*, vol. 23, no. 1, pp. 524–552, 2021, doi: 10.1109/COMST.2020.3036778.

[42] Y. Uhm and W. Pak, "Service-Aware Two-Level Partitioning for Machine Learning-Based Network Intrusion Detection with High Performance and High Scalability," *IEEE Access*, vol. 9, pp. 6608–6622, 2021, doi: 10.1109/ACCESS.2020.3048900.

[43] S. Sharma, P. Zavarsky, and S. Butakov, "Machine Learning based Intrusion Detection System for Web-Based Attacks," *Proc. - 2020 IEEE 6th Intl Conf. Big Data Secur. Cloud, BigDataSecurity 2020, 2020 IEEE Intl Conf. High Perform. Smart Comput. HPSC 2020 2020 IEEE Intl Conf. Intell. Data Secur. IDS 2020*, pp. 227–230, 2020, doi: 10.1109/BigDataSecurity-HPSC-IDS49724.2020.00048.

[44] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *J. Inf. Secur. Appl.*, vol. 50, p. 102419, 2020, doi: 10.1016/j.jisa.2019.102419.

[45] F. Ertam, "An efficient hybrid deep learning approach for internet security," *Phys. A Stat. Mech. its Appl.*, vol. 535, p. 122492, 2019, doi: 10.1016/j.physa.2019.122492.

[46] F. K. Tsai, C. C. Chen, T. F. Chen, and T. J. Lin, "Sensor Abnormal Detection and Recovery Using Machine Learning for IoT Sensing Systems," *2019 IEEE 6th Int. Conf. Ind. Eng. Appl. ICIEA 2019*, pp. 501–505, 2019, doi: 10.1109/IEA.2019.8715215.

[47] A. Salem and S. Banescu, "Metadata recovery from obfuscated programs using machine learning," *ACM Int. Conf. Proceeding Ser.*, vol. 05-06-December-2016, 2016, doi: 10.1145/3015135.3015136.

[48] J. Canedo and A. Skjellum, "Using machine learning to secure IoT systems," *2016 14th Annu. Conf. Privacy, Secur. Trust. PST 2016*, pp. 219–222, 2016, doi: 10.1109/PST.2016.7906930.

[49] A. I. Abubakar, H. Chiroma, S. A. Muaz, and L. B. Ila, "A review of the advances in cyber security benchmark datasets for evaluating data-driven based intrusion detection systems," *Procedia Comput. Sci.*, vol. 62, no. Scse, pp. 221–227, 2015, doi: 10.1016/j.procs.2015.08.443.

[50] A. V. Sukhanov, S. M. Kovalev, and V. Stýskala, "Advanced temporal-difference learning for intrusion detection," *IFAC-PapersOnLine*, vol. 28, no. 4, pp. 43–48, 2015, doi: 10.1016/j.ifacol.2015.07.005.

[51] P. Wang and Y. S. Wang, "Malware behavioural detection and vaccine development by using a support vector model classifier," *J. Comput. Syst. Sci.*, vol. 81, no. 6, pp. 1012–1026, 2015, doi: 10.1016/j.jcss.2014.12.014.

[52] D. P. Gaikwad and R. C. Thool, "Intrusion detection system using Bagging with Partial Decision Tree base classifier," *Procedia Comput. Sci.*, vol. 49, no. 1, pp. 92–98, 2015, doi: 10.1016/j.procs.2015.04.231.

[53] H. Zhang, D. Yao, N. Ramakrishnan, and Z. Zhang, "Causality reasoning about network events for detecting stealthy malware activities," *Comput. Secur.*, vol. 58, no. May 2012, pp. 180–198, 2016, doi: 10.1016/j.cose.2016.01.002.

[54] S. Liu, Y. Wang, J. Zhang, C. Chen, and Y. Xiang, "Addressing the class imbalance problem in Twitter spam detection using ensemble learning," *Comput. Secur.*, vol. 69, pp. 35–49, 2017, doi: 10.1016/j.cose.2016.12.004.

[55] P. Li *et al.*, "Multi-key privacy-preserving deep learning in cloud computing," *Futur. Gener. Comput. Syst.*, vol. 74, pp. 76–85, 2017, doi: 10.1016/j.future.2017.02.006.

[56] A. Li, J. Wu, and Z. Liu, "Market Manipulation Detection Based on Classification Methods," *Procedia Comput. Sci.*, vol. 122, pp. 788–795, 2017, doi: 10.1016/j.procs.2017.11.438.

[57] D. X. Cho, D. T. H. Thuong, and N. K. Dung, "A Method of Detecting Storage Based Network Steganography Using Machine Learning," *Procedia Comput. Sci.*, vol. 154, pp. 543–548, 2018, doi: 10.1016/j.procs.2019.06.086.

[58] E. G. Dada, J. S. Bassi, H. Chiroma, S. M. Abdulhamid, A. O. Adetunmbi, and O. E. Ajibuwa, "Machine learning for email spam filtering: review, approaches and open research problems," *Heliyon*, vol. 5, no. 6, 2019, doi: 10.1016/j.heliyon.2019.e01802.

[59] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet of Things*, vol. 11, p. 100227, 2020, doi: 10.1016/j.iot.2020.100227.

[60] D. Yu, J. Kang, and J. Dong, "Service Attack Improvement in Wireless Sensor Network Based on Machine Learning," *Microprocess. Microsyst.*, vol. 80, no. December 2020, p. 103637, 2021, doi: 10.1016/j.micpro.2020.103637.

[61] O. K. Sahingoz, E. Buber, O. Demir, and B. Diri, "Machine learning based phishing detection from URLs," *Expert Syst. Appl.*, vol. 117, pp. 345–357, 2019, doi: 10.1016/j.eswa.2018.09.029.